Digital Signatures Initiative

Final Report of the DSI Workgroup
Council on Technology Services
Commonwealth of Virginia

October 2000

VOLT

Virginia On-Line Transaction Certificates:

An Enterprise Solution of Trust

Digital *Signatures* INITIATIVE:
AN ENTERPRISE SOLUTION OF TRUST

I.

Final Report of the DSI Workgroup

October 2000

Prepared for

The Council on Technology Services
Commonwealth of Virginia

By

The COTS Digital Signatures Initiative Workgroup

Cheryl Clark
Chair

R. F. “Chip” German
Vice Chair

October 30, 2000

Dear Colleague:

I am pleased to share with you *Virginia On-Line Transaction Certificates: An Enterprise Solution of Trust*, which marks the culmination of the DSI Workgroup's findings, conclusions, recommendations, and plan of action. Our report aims to capture the depth and breadth of activities conducted in a compact timeframe and to fuel the deployment effort. The Workgroup has proposed a comprehensive, synergistic approach to digital signatures deployment on an aggressive timetable.

Recognizing the full spectrum of security options, the Privacy, Security, and Access Workgroup of the Council on Technology Services (COTS) charged the Digital Signatures Initiative (DSI) Workgroup with examining digital signatures—a form of electronic signature—for the Commonwealth of Virginia. First convened in December 1999, the DSI Workgroup has vigorously pursued its charge in a relatively brief period of time. Over the last 11 months, the Workgroup has:

- Launched eleven digital signatures with public key infrastructure (PKI) pilot demonstration projects that were more robust than most digital signatures deployments.
- Sponsored "Education Day" for more than 70 participants to provide in-depth information on digital signatures deployment considerations and solidify plans for the pilot demonstrations.
- Leveraged the best thinking and expertise of the vendor community and leaders of other digital signatures deployments, including the federal government, the Government of Canada, other states, and private industry.
- Developed a comprehensive body of lessons learned and best practices to fuel the deployment effort in the Commonwealth of Virginia.
- Met in monthly sessions to exchange information and lessons learned.

Our plan was presented to COTS during the Commonwealth of Virginia Information Technology Symposium (COVITS) on September 27, 2000, and commissioned to move forward pending review of the final report at the November 13 COTS meeting. Copies of the Final Report and Executive Summary are available on the COTS Digital Signatures Initiative web site, at http://www.sotech.state.va.us/cots/dsi.

Some caveats. Digital signature technology continues to evolve and mature rapidly. Though this report marks the close of this phase of our work together, it is not a closed book. Rather, it captures a snapshot of our conclusions about digital signatures as of October 2000. Our thinking continues to evolve and mature as we move into the deployment stage and explore opportunities for linking to other models and programs promulgated by national and international organizations.

Next steps. The DSI Workgroup is in the process of evolving into the Digital Signature Deployment Workgroup. I am pleased to announce the creation of the following teams and team leaders who will ably lead us forward in the coming months:

- *VOLT Governance Team—Chip German, Director of Policy and Planning, University of Virginia.* The VOLT Governance Team will recommend policies, standards, and guidelines to the Secretary of Technology that will govern all aspects of certificate structure and management, including determination of VOLT Early Adopters.
- *Procurement Team—Jim Adams, Senior Information Technology Manager, Department of Information Technology.* The Procurement Team will recommend strategies for acquiring digital signature products and services and to support enterprise-wide availability.
- *Audit & Assurance Team—Barbara Deily, Director of Audits, University of Virginia.* The Audit & Assurance Team will provide guidance in the areas of audit and control standards, legal issues and liability, and finance and accounting.
- *Emerging Technology Team—Sally Fehn, Security Division Consultant, Department of Information Technology.* The Emerging Technology Team will explore technologies and standards that are new or under development for inclusion in Virginia's solution.
- *Business Connections Team—Shirley Payne, Director of Security Coordination & External Relations, University of Virginia.* The Business Connections Team will explore national and international models, programs, and initiatives that may provide opportunities for mutually beneficial partnerships with other organizations.
- *Education and Promotion Team—Electronic Government Implementation Division.* The Education and Promotion Team will provide education and training to build awareness about and familiarity with digital signatures and perform outreach to agencies, institutions, and localities to increase involvement and participation.

Sincerely,

Cheryl Clark, Chair
Digital Signatures Initiative Workgroup

cc: The Honorable Donald W. Upson

DIGITAL SIGNATURES INITIATIVE WORKGROUP

MEMBERS

Jim Adams
Sr. Information Technology Manager
Department of Information Technology

David Bunn
Network Systems Supervisor
Department of Motor Vehicles

Charles Cassaro
Team Supervisor
City of Norfolk

Cheryl Clark (Chair)
Chief Information Officer
Department of Motor Vehicles

Jan Fatouros
Director of Information Systems & Services
Department of General Services

Chip German (Vice Chair)
Director of Policy & Planning
University of Virginia

Sandy Graham
Data Security Administrator
County of Chesterfield

Diane Horvath
Director of Marketing
Virginia Interactive, LLC

Jack Kennedy
Clerk of the Court
County of Wise

Virgil Kopf
CIO Information Management Systems
Department of Game & Inland Fisheries

Ray Lindquist
Vice President - Business Systems
Parikh Advanced Systems for
Department of Transportation

Tom Loper
Applications Development Specialist
Virginia Information Providers Network

Jim MaGill
Information Protection Manager
County of Fairfax

Dave Molchany
Chief Information Officer
County of Fairfax

Murali Rao
Director, Data Management Division
Department of Transportation

Wayne Robertson
Director, MIS Division
Department of Information Technology

Bill Russell
Deputy Director
County of Chesterfield

Tim Sigmon
Director, Advanced Technology
University of Virginia

Arnold Thielen
President, Mixnet Corporation for
County of Wise

Ron Tokarcik
Information Systems Analyst
City of Norfolk

AUDIT & ASSURANCE TEAM

John Breeden
Manager, Records Analysis Section
Library of Virginia

Rick Cooke
Internal Audit Manager
Department of Transportation

Al Carpenter
Internal Audit Director
Department of Motor Vehicles

Barbara Deily (Chair)
Director of Audits
University of Virginia

Ben Herman (Vice Chair)
Internal Audit Director
Department of Information Technology

Charles Lawver
Internal Audit Director
Department of Medical Assistance Services

Margaret Maupin
Internal Audit Director
Department of General Services

John Moore
Accounting Manager
Department of Game & Inland Fisheries

Shirley Payne
Director, External Relations & Security Coordination
University of Virginia

Bob Ross
EDP Auditor
County of Chesterfield

Kevin Savoy
Auditor
Auditor of Public Accounts

Ben Sutphin
Internal Audit Supervisor
Department of State Internal Auditor

Glenn Thacker
IT Internal Audit Manager
Department of Taxation

Steven VonCanon
Manager, Disbursements Review and Fixed Assets
Department of Accounts

STAFF

Janice Akers, Research and Project Coordination
Vivian Cheatham, Administrative Support
Cleo Rehmer, Research and Project Coordination
Jennifer Wootton, Technical Writer

DSI WORKGROUP CONTRIBUTORS

Sprio Alifrangis
Baltimore Technologies

Gerry Anderson
Entrust Technologies

Emily Atkinson
Entrust Technologies

Jim Banwell
CACI

Becky Barnett
Department of General Services

Tim Bass
Virginia Retirement System

Roslynne Blake
Computer Associates

Michael Boorom
Operational Research Consultants, Inc.

Jim Brandt
VeriSign

Leslie Carter
Department of Information Technology

Phil Camero
Performance Engineering Corporation

Lisa Coates
Century Date Change Initiative Project Office

Claudine Conway
Government Technology Services, Inc.

Alan Cordaro
Computer Associates

David Corry
VeriSign

Mark Davis
Network Associates, Inc.

Mark Dennis
Operational Research Consultants, Inc.

David Dobson
Entrust Technologies

Debbie Dodson
Department of Motor Vehicles

Sally Fehn
Department of Information Technologies

Sandy German
University of Virginia

Richard Gill
RSA Security

Craig Goeller
Department of Medical Assistance Services

Debra Goodman
Computer Associates

Tom Greco
Digital Signature Trust Company

Frank Guinan
CACI for Department of Medical Assistance Services

Richard Guida
(Chair) Federal PKI Steering Committee

Gary Gumm
Parikh Advanced Systems

Michael Horkey
Unisys Corporation

John Jung
Joint Commission on Technology and Science

Lynn Kinch
Performance Engineering Corporation

Mark Kneidinger
Electronic Government Implementation Division

Yuriy Kzambasow
Digital Signature Trust Company

Chris Law
KPMG

Joe Lilly
(former) Department of General Services

Thomas Moody
Department of Information Technology

Tim Moses
Entrust Technologies

Frederick Norman
(former) Unisys Corporation

Nick Otto
Parikh Advanced Systems

Don Parr
KPMG

Brian Pierce
KPMG

Andy Poarch
(former) Executive Director, Council on Technology Services

Lee Reams
City of Norfolk

Jake Reynolds
Department of Information Technology

Stephanie Saccone
Department of Information Technology

Rose Schooff
Library of Virginia

Lana Shelley
Department of Motor Vehicles

Lynn Sikora
Department of Game & Inland Fisheries

Susan Martin
Department of Information Technology

Prasanna Simha
Computer Associates

Ann Smith
Valicert, Inc.

Michael Snipes
Entrust Technologies

Jeff Stapleton
KPMG

David Sweigert
Entrust Technologies

Rusty Taub
RSA Security

Teresa Thomas
Auditor of Public Accounts

Danny Wasyk
County of Chesterfield

Brandon Weidner
Computer Associates

Karen West
Digital Signature Trust Company

Richard Wilhelm
County of Fairfax

Rodney Willett
Virginia Information Providers Network

PARTICIPATING GOVERNMENT AND INDUSTRY ORGANIZATIONS

Auditor of Public Accounts, Commonwealth of Virginia
Baltimore Technologies
CACI
Cardobe Technologies
City of Charlottesville
City of Norfolk
Computer Associates
Council on Technology Services, Commonwealth of Virginia
County of Chesterfield
County of Fairfax
County of Wise
Department of Accounts, Commonwealth of Virginia
Department of Game & Inland Fisheries, Commonwealth of Virginia
Department of General Services, Commonwealth of Virginia
Department of Information Technology, Commonwealth of Virginia
Department of Medical Assistance Services, Commonwealth of Virginia
Department of Motor Vehicles, Commonwealth of Virginia
Department of State Internal Auditor, Commonwealth of Virginia
Department of Taxation, Commonwealth of Virginia
Department of Transportation, Commonwealth of Virginia
Digital Signature Trust Company
Electronic Government Implementation Division, Commonwealth of Virginia
Entrust Technologies
Federal PKI Steering Committee
Government Technology Services, Inc.
Joint Commission on Technology & Science, Commonwealth of Virginia
KPMG
Library of Virginia, Commonwealth of Virginia
Mixnet Corporation
Network Associates, Inc.
NIC Commerce
Operational Research Consultants, Inc.
Parikh Advanced Systems
Performance Engineering Corporation
RSA Security
SAGA
Unisys Corporation
University of Virginia
Valicert, Inc.
VeriSign
Virginia Information Providers Network
Virginia Retirement System

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

INTRODUCTION

The promise and potential of the Information Age offers a vast range of opportunities for fundamentally changing and improving the way citizens and businesses interact with government and their communities. As the "Internet Capitol of the World," the Commonwealth of Virginia has passed critical legislation, including the nation's first Uniform Electronic Transactions Act (UETA), and issued substantive directives to help agencies reap the benefits of conducting government business in the electronic world. As Commonwealth agencies build on UETA and embrace new technologies to improve customer convenience, increase worker productivity, and benefit from significant time and cost savings, they seek to foster an electronic environment of trust.

A foundation of trust. Digital signatures are one form of electronic signatures. Digital signatures legally bind individuals to specific transactions by relying on technology (i.e., public key cryptography) and policy (i.e., rigorous registration processes and criteria). Like passports, digital certificates—which vouch for digital signatures—are issued by trusted third parties, known as certification authorities (CAs), and can be used to provide high levels of assurance and foster an environment of trust in the electronic world.

An enterprise solution. The Council on Technology Services (COTS) charged the Digital Signatures Initiative (DSI) Workgroup in Winter 1999 with the following deliverables:

- The foundation of policies, practices, guidelines, and standards necessary to transition into an enterprise technical production environment.
- An enterprise technical architecture and acquisition strategy based on experience.
- A Commonwealth Bridge Certification Architecture.
- An invested knowledge and skills base for decision makers and technical staff.
- A demonstrated working solution of trust and confidence extensible to the Commonwealth public sector community, to business partners, and to the public.

Workgroup participants and contributors. The DSI Workgroup is comprised of representatives from five agencies, five localities, University of Virginia, and VIPNet (Virginia Interactive, Inc). The DSI Workgroup established an Audit & Assurance Team—comprised of auditors and security professionals—to identify administrative obstacles, develop a digital signatures decision model, review standards, and develop an audit and control framework. The DSI Workgroup also benefited from the knowledge and experience of Commonwealth employees and contractors, the vendor community, other states, the Federal government, and the Government of Canada.

The process. To get a jumpstart, the DSI Workgroup leveraged the best thinking and experiential learning of other states, the Federal government, and the private sector. The DSI Workgroup first convened in December 1999, and conducted monthly business meetings to share information on best practices and methods for overcoming barriers and obstacles.

The Workgroup launched eleven digital signature with public key infrastructure (PKI) demonstrations in Summer 2000, and used the lessons learned from the demonstration effort to inform its findings and recommendations. The University of Virginia conducted a limited and successful demonstration of a bridge certification authority (BCA). The BCA is modeled after the federal bridge project, and cross-certifies certification authorities (CAs) to promote interoperability and expand trust domains.

VISION AND GUIDING PRINCIPLES

The DSI Workgroup supports the Governor's vision for The Digital Dominion—for improved, efficient operation of government and greater convenience and delivery of government services to citizens and businesses. The DSI Workgroup envisions creating an environment of trust, interoperability, and security for individuals and businesses conducting electronic transactions with the Commonwealth of Virginia.

Guiding principles. The DSI Workgroup built consensus around the following guiding principles, which provided a sound framework for the subsequent recommendations:

- *The power of attraction*. Create a voluntary, Commonwealth enterprise solution that will garner support and widespread use among agencies, institutions, and localities, not because it is compulsory, but because it is attractive, maximizes convenience for internal and external customers, optimizes ease of adoption and use, and makes the best business sense.
- *A solid foundation.* Our recommendations are framed to ensure integrity, flexibility, and maximum security balanced with the pace and scope of deployment. We want to build a solid foundation to position the Commonwealth to take advantage of the greatest gains in the rapidly-evolving technology marketplace.
- *Simplicity and flexibility.* To achieve early deployment and facilitate ease of adoption and use for agencies, institutions, and localities, our recommendations aim for the simplicity of the "cleanest," least complicated and most flexible technology and policy solutions.

FINDINGS AND CONCLUSIONS

Our substantial body of findings, lessons learned, and best practices has led us to draw the following seven key conclusions:

1. **Trust is the linchpin of digital signature technology.** Trust is absolutely central to digital signatures. The highest level of assurance is necessary to conduct trustworthy electronic transactions with confidence.

2. **Digital signatures should be used for authentication, data integrity, and non-repudiation.**

3. **Digital signature technology has a place in an overall security architecture.** Digital signatures are one form of electronic signing and one form of authentication. Digital signatures in and of themselves do not provide the basis for e-government. An absence of digital signature capability in the hierarchy of electronic signatures, however, can be an impediment to e-government. For applications involving high risks and extremely sensitive data, and requiring a high level of assurance that the parties involved in the transactions are who they claim to be, digital signature solutions are unparalleled.

4. **Deploying digital signature technology is not a trivial exercise.** The demonstration effort confirmed that digital signatures and PKI are far from being "plug and play" solutions. Implementation involves:
    - Significant investment of time, resources, and expertise;
    - A steep learning curve;
    - Substantial process reengineering;
    - Overcoming cultural, legislative, technical, and policy barriers;
    - Evolving standards;
    - Interoperability issues; and
    - Open questions of liability.

5. **Digital signature and electronic government deployments are subject to systemic obstacles that can create a cycle of paralysis.** Transitioning to an e-government environment turns the "business as usual" (or "government as usual") paradigm on its ear. Systemic obstacles to this re-thinking exist, such as:
    - Infrastructure
    - Cultural beliefs and practices

- Funding
- Staffing

Effecting change in the fundamental way in which government conducts business requires breaking the cycle of systemic problems and gaining a critical mass of acceptance and support.

6. **The greatest value of digital signatures lies in associated reengineering of business processes.** The greatest potential value may derive from the process of reengineering workflow and applications to create a customer-oriented electronic environment. Digital signatures and automation present opportunities to raise standards for business processes, workflow, and security and improve and redefine best practices. We want to put a working philosophy in place that we not replicate the security and accountability weaknesses and vulnerabilities often inherent in paper-based processes as we transition these processes into the electronic world.

7. **Digital signatures are connected to and can advance other Commonwealth initiatives and activities toward a seamless implementation of electronic government.** The progress of the DSI Workgroup interrelates with Executive Orders 51 and 65 and with other initiatives spearheaded by COTS, the Secretary of Technology, and his reporting agencies. In particular, the work of the following groups or initiatives provides specific opportunities to create synergies:
   - COTS Privacy, Security and Access Workgroup
   - COTS Enterprise Architecture/Security Workgroup
   - Department of Technology Planning
   - EO 51 E-forms and digital signatures
   - EO 65 Administrative Systems
   - COTS Seat Management Program
   - Commonwealth Portal Strategy
   - Commonwealth Kiosks

SUMMARY CONCLUSION

Relying on the guiding principles and findings and conclusions articulated by the DSI Workgroup, the Commonwealth should deploy digital signature and PKI technology strategically. Recognizing the legal, policy, technical, operational, cultural barriers; uncertainties related to applied case law; and the continued evolution of associated standards and products, the Commonwealth should move forward strategically to build momentum and the infrastructure that would support a full-scale PKI production environment. To that end, the DSI Workgroup believes the Commonwealth should adopt an enterprise solution of trust—a solution that offers a wide array of digital signature and PKI products, provides flexibility and simplicity, and promotes interoperability.

RECOMMENDATIONS

The Workgroup has crafted numerous recommendations to support implementation of digital signatures. The top ten recommendations include:

1. **Issue Virginia On-Line Transaction (VOLT) Certificates.**

   To ensure interoperability, portability, and simplicity, the Workgroup recommends issuing VOLT Certificates that adopt open standards, provide high levels of assurance, and would be used for identity only. Individuals could use VOLT Certificates with participating agencies, institutions, and localities, thereby lifting substantial key management burdens from the user. Open standards are vendor-neutral, and promote interoperability among multiple CAs.

   In the initial stages of deployment, the Workgroup recommends issuing high assurance certificates only to ensure users understand the need to maintain absolute control over their private signing keys. The Workgroup recommends instituting a Commonwealth PIN in the place of low assurance certificates.

2. **Develop and deploy interoperability mechanisms.**

   To foster a multi-layered, multiple-vendor environment, the Commonwealth must explore and deploy interoperability mechanisms (such as bridges and meta-directories) to expand domains of trust. High assurance certificates issued by other governmental entities—such as the U.S. Department of Defense—could be reviewed and accepted by the VOLT Governance Team to be used alongside the VOLT Certificate. The Workgroup also recommends that the Commonwealth monitor emerging guidelines and standards at the international and national levels.

3. **Involve legal counsel that understands the technology to advise on issues of liability and legality and assists to advance the Administration's goals for The Digital Dominion.**

   The Workgroup recommends the Office of the Attorney General consider creating, administratively or through legislation, a Division of Electronic Government to provide dedicated advice and assistance to all agencies and institutions of the Commonwealth. This new division in the Office of the Attorney General is analogous to the Division of Consumer Counsel (sec. 2.1-133.1) and the Division of Debt Collection (sec. 2.1-133.4). The purpose of establishing a dedicated legal division is to provide the technological/legal expertise necessary to guide the Commonwealth's agencies and institutions through the cutting edge issues that characterize e-government at a pace that supports a leadership position for the Commonwealth.

4. **The Department of Information Technology, with direction from the Secretary of Technology and the support of the Electronic Government Implementation Division (eGov), should develop and manage the procurement of digital signature-related products and services for use by agencies, institutions, and localities.**

   The Workgroup recommends out-sourcing the certification authority (CA) function to leverage industry expertise and hasten deployment. To ensure a multi-layered environment with multiple CAs, the Workgroup recommends contracting with an enterprise PKI services coordinator that will work with multiple vendor products and solutions and provide technical assistance.

   The Workgroup recommends that the RFP(s) address provisioning the following key areas:

   - CA products and services
   - Interoperability mechanisms (such as a bridge CA)
   - Commonwealth PIN management
   - Application and platform integration products and services
   - Education and training
   - Marketing and promotion
   - Document retention and recovery mechanisms

5. **Reconfigure the DSI Workgroup and establish the Digital Signature Deployment Team to provide governance and policy and implementation oversight.**

   The Workgroup should be reconfigured to match the new proposed deployment effort. This will include legal assistance from the Office of the Attorney General and designation of five teams: the VOLT Governance Team, Procurement Team, Audit & Assurance Team, Emerging Technologies Team, Business Connections Team, and Education and Promotion Team.

6. **Provide resources and support for agency, institution, and local government adoption of PKI and digital signatures.**

   The Workgroup recommends providing seed money, resources, and other incentives to promote use of digital signature technology.

7. **Connect with Commonwealth initiatives and activities to promote a unified, synergistic approach to electronic government implementation.**

   The Workgroup recommends building on opportunities from Executive Orders 51 and 65 to boost electronic government and deploy electronic and digital signatures. Agencies and institutions should follow the Secretary of Technology's guidance per EO 51 in incorporating electronic and digital signatures into their applications. The Workgroup recommends considering administrative applications, as defined in EO 65, as candidates for digital signature technology.

8. **Launch the VOLT Early Adopters Program for agencies, institutions, and localities that are willing and capable to deploy digital signatures in a production environment.**

   Modeled after the Washington Early Adopters and Illinois' Seed Certs programs, the VOLT Early Adopters Program will demonstrate success in G2G, G2B, and G2C applications, boost confidence, and build momentum for future deployments. The outcome of the initiative will be a solid infrastructure that will support the use of digital signatures for electronic government applications in the Commonwealth of Virginia.

9. **Provide education and training to build awareness about and familiarity with digital signature technology and its benefits and implementation decision factors.**

   Conduct an education and awareness campaign targeted to Commonwealth employees in agencies, institutions, and localities; legislators; and segments of the business and citizen populations. All digital signature users should receive security awareness training for private key protection before high-assurance key pairs are issued. All digital signature users should formally acknowledge their responsibilities for protecting their private key before access to any system utilizing the high-assurance key is granted.

10. **Leverage the learning and expertise of others, and monitor emerging technologies and security solutions for applicability to the Commonwealth.**

    Because the environment continues to evolve rapidly and operates in a larger context than a single entity, region, state, or country, there are significant opportunities for linking, leveraging, and leadership on the horizon.

    Emerging Applications and Practices

    - Health Insurance Portability and Accountability Act (HIPAA)
    - Electronic notaries
    - Voter registration and online voting applications
    - New business models
    - Federal Access Certificates for Electronic Services (ACES) program
    - Department of Motor Vehicles as the state's Registration Authority (RA)

    Evolving Standards and Technologies

    - Electronic forms and workflow software
    - Biometrics
    - Smartcards and alternative hardware tokens
    - Encryption
    - Document management.
    - Tools and methodologies that could enable Single Sign On (e.g., directory structures, attribute certificates, privilege management frameworks, etc.)

PLAN OF ACTION

The DSI Workgroup recommends the following action steps.

1. The Secretary of Technology should reestablish the Digital Signatures Workgroup to consist of the VOLT Governance Team, the DS Procurements Team, the Horizons Team, and the Audit & Assurance Team and other sub-units to support the proposed deployment effort. The new DS Deployment Workgroup should oversee the RFP development process and coordinate the resolution of legal, policy, and technical issues

   Timeframe: October 2000

2. DIT should procure a vendor source or sources for an array of enterprise products and services related to PKI and digital signatures, including CA services (prominently featuring VOLT-standard products) and all based on DSI findings and recommendations. DIT should work with the DS Procurement Team to develop a concept of operations and articulate the VOLT open standards. Applications and platform integration services should be procured in the same manner.

   RFP Development: October 2000 – January 2001
   Issue RFP(s): January 2001
   Award RFP(s): June/July 2001

3. The standards and best practices recommended by the DSI Workgroup should be adopted through the Secretary of Technology, most notably those applying to the VOLT Certificate, its assurance levels, audits and controls, storage of private keys, and recommended limits on the use of document encryption for storage.

   October 2000

4. A source of funding should be sought by the Secretary of Technology.

   October 2000

5. Appropriate staffing should be supplied for the effort through the Secretary of Technology, most notably legal counsel and project management.

   October –November 2000

6. The proposed digital signature deployment timeline should be adopted by and promoted as a priority to Secretary of Technology agencies.

   October 2000 – January 2001

7. Early Adopter candidates—Executive Order 65 administrative applications, agencies, localities, and the educational community—should be recruited selectively by the Digital Signature Deployment Workgroup and commissioned by the Secretary of Technology.

   October 2000 – January 2001

8. The COTS Executive Committee should proactively exploit synergies the Digital Signatures Initiative has identified with other COTS initiatives and align priorities and resources to boost momentum toward the Administration's vision for the Digital Dominion.

   October 2000 and ongoing

9. The Department of Technology Planning and the Electronic Government Implementation Division should develop a training program and a promotional and security awareness campaign that takes advantage of the DSI findings and lessons learned.

   October 2000 – January 2001

10. The DS Horizons Team should actively monitor 'horizon' issues and work through COTS to adjust for and to leverage these developments.

    October 2000 and ongoing

TOOLS AND RESOURCES

As a result of the DSI effort, we have developed a number of tools and guidelines, and developed a substantial base of knowledge to advance the Commonwealth toward the Governor's vision for The Digital Dominion. In particular, we have:

Solutions

- A simplified, vendor-neutral trust architecture model based on open standards.
- A flexible business model to guide implementation of digital signatures that can meet the needs of the Commonwealth as an enterprise as well as the needs of its disparate organizational components.
- Principal role definitions for moving forward in a coordinated, strategic manner with multiple partners.

- An acquisition strategy with selected supporting reference materials to inform and guide deployment decisions.
- A plan of action synergistic with other COTS endeavors and initiatives at all levels in the public and private sectors.
- An enterprise solution to offer agencies, localities, and higher education that provides the best business case for adopting digital signature technology.

Tools

- Step-by-step business decision criteria to guide decision-makers in determining whether digital signature technology is appropriate.
- A cost model that highlights direct and opportunity costs, and the major cost considerations in deploying digital signature technology.
- Audit and assurance best practices and standards to ensure proper controls are put into place to protect transactions, prevent fraud, and provide an audit trail.
- Key technical standards to promote interoperability and provide high levels of assurance.

Resources

- Experience-based knowledge and skills developed through the robust demonstration effort and by building on the knowledge and experiences of others nationally and internationally.
- An informed perspective on evolving issues and trends.
- Contacts in multiple states, the federal government, and the Government of Canada.
- Strong industry relationships with digital signature and PKI vendors and experts.

Conclusion. As a result of the DSI Workgroup's inquiry, the Commonwealth of Virginia is positioned to assume a leadership role in deploying digital signature technology strategically to improve services to citizens, realize cost-savings benefits, and reap the benefits of electronic government.

II. INTRODUCTION

Vision for The Digital Dominion: "To create a technology environment such that every citizen in every aspect of their daily life, be it economic, educational or personal, and in every interaction with government, is fully empowered by and benefits from, the promise and potential of the Information Age."

—Governor Jim Gilmore

The promise and potential of the Information Age offers a vast range of opportunities for fundamentally changing and improving the way citizens and businesses interact with government and their communities. As the "Internet Capitol of the World," the Commonwealth of Virginia is committed to ensuring all Commonwealth citizens, businesses, and employees benefit from the convenience, efficiency, and opportunity afforded by the Internet. The Commonwealth has passed critical legislation, including the nation's first Uniform Electronic Transactions Act (UETA), and issued substantive directives to help agencies reap the benefits of conducting government business in the electronic world.

A life of its own. The Internet and the World Wide Web have experienced the greatest growth of any other technology. It took the telephone 38 years to penetrate 30% of all U.S. households and the television 17 years. The Web took less than seven years. Approximately $66 billion in electronic commerce was conducted last year, and estimates show that the online spending trend is increasing rapidly. The Internet continues to grow at a rate of about 40% to 50% each year in terms of number of machines connected.[1]

How big is the Internet?[9]

Number of host computers
More than 56 million in 247 countries

Number of Web pages
More than 1 billion

Number of servers
More than 6.4 million

Estimated online retail sales (1999)
$66 billion

Pages with .com extension
54.68%

Pages with .gov extension
1.15%

Percentage of pages in English
86.55%

Three physicists from Notre Dame have measured the connectivity of the Internet and found that the average web page has seven links to other pages. According to their study, a large number of web pages have a huge number of connections—far more than they anticipated based on traditional mathematical models. In studying the Internet's topology and growth dynamics, the researchers determined that the web follows a power law in physics:

> "'A power law distribution means that the web doesn't follow the usual mathematical models of random networks, but instead exhibits the type of physical order found in… magnetic fields, galaxies, and plant growth.' Thus, the web seems to have taken on an organic life of its own.[2]

Electronic commerce and electronic government. What are the benefits of electronic commerce and electronic government (e-government)? According to the U.S. Department of Commerce, the Internet is a tool for "providing more useful information, expanding choice, developing new services, streamlining processes, and lowering costs.[3]"

Vision for e-government in the Commonwealth of Virginia. According to the vision Governor James Gilmore set out in Executive Order 65, e-government will enable citizens and businesses to interact with a more streamlined, service-oriented government:

> "In this environment, citizens and businesses will not simply receive information or participate in transactions passively. Rather, they will become involved in a more active dialog with their state government. Successful e-government will be achieved when all Virginia's citizens and communities are efficiently using the tools of technology, especially the Internet, to actively participate in their state government.[4]"

Virginia Leadership. The Commonwealth of Virginia is at the forefront of technology initiatives. Recognized for his achievements in advancing technology initiatives in Virginia, Governor Gilmore chaired the Congressional Advisory Commission on Electronic Commerce. The Commission recommended national taxation policies to stimulate Internet growth and allow all citizens to realize the social and economic benefits of the Internet.

In the Commonwealth of Virginia, Governor Gilmore issued Executive Orders 51 and 65, requiring all executive branch agencies to web-enable their forms and to transition services to an electronic environment. Digital signatures were cited specifically as one of six key initiatives foundational to implementing electronic government. Gilmore also appointed Donald W. Upson as the first cabinet-level Secretary of Technology position in the nation, and developed the Electronic Government Implementation Division (eGov) to assist agencies, institutions, and localities with the design and implementation of e-government initiatives. Most recently, Governor Gilmore established The Digital Dominion in September 2000. The Digital Dominion is a model for governance during the Internet age, and is intended to bring all citizens and businesses together to maximize the potential of the Internet and communications technologies.

A foundation of trust. As Commonwealth agencies build on the Governor's vision and UETA and embrace new technologies to improve customer convenience, increase worker productivity, and benefit from significant time and cost savings, they seek to foster an electronic environment of trust. Highly publicized events, such as identity fraud and breaches in security resulting in the compromise of confidential information, disruption of services, and destruction of data and systems, have created worldwide concerns over security of conducting business online. According to experts, distrust is the primary reason why individuals choose not to conduct transactions online—when I cannot see you, how do I know you are who you say you are?

Signatures. Digital signatures are one form of electronic signatures. According to the Federal Electronic Signatures in Global and National Commerce Act of 2000, an electronic signature is "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.[5]"

VIRGINIA: BIRTHPLACE OF THE INTERNET

Percentage of households with Internet access (1998)
735,000 (27.9%)[10]

Infrastructure
More than 650,000 miles of fiber-optic cable—more than any other state.

High technology
More than 4,700 high-tech firms employing 158,000 Virginians.
Virginia ranks 3rd in the nation and 1st on the east coast for number of employees in advanced telecommunications services.

Internet-related business
More than 3,000 information technology, telecommunications, and Internet companies.

Internet traffic
More than 50% of all Internet traffic passes through Virginia.[11]

According to the American Bar Association, a written signature, or "wet signature," is any mark made with the intention of authenticating the marked document.[6]" Signatures serve the following purposes:

- "**Evidence**: A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
- **Ceremony**: The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent 'inconsiderate engagements.'
- **Approval**: In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect.
- **Efficiency and logistics**: A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document.[7]"

Digital signatures. Digital signatures are like an electronic passport. In the physical world, your passport and thus your identity is "vouched for" by the U.S. Department of State. When you arrive in another country, the officials trust that the U.S. Passport Office has verified—or authenticated—your identity. Though the official may not know you, he or she relies on the integrity of the U.S. Government and can trust that you are who you say you are.

Like passports, digital certificates are issued by trusted third parties, known as certification authorities (CAs). Digital signatures legally bind individuals to specific transactions by relying on technology (i.e., public key cryptography) and policy (i.e., rigorous registration process and criteria). Thus, you can authenticate yourself to a system or another user. Digital signatures can be used to provide high levels of assurance and foster an environment of trust in the electronic world. (See *Overview of Digital Signatures and PKI* for more information.)

Digital signatures can be used to provide high levels of assurance and foster an environment of trust in the electronic world.

An enterprise solution. Recognizing the necessity for and benefits of digital signatures in the Commonwealth, the Council on Technology Services (COTS) charged the Digital Signatures Initiative (DSI) Workgroup in Winter 1999 with the following deliverables:

- The foundation of policies, practices, guidelines, and standards necessary to transition into an enterprise technical production environment.
- An enterprise technical architecture and acquisition strategy based on experience.
- A Commonwealth Bridge Certification Architecture.
- An invested knowledge and skills base for decision makers and technical staff.
- A demonstrated working solution of trust and confidence extensible to the Commonwealth public sector community, to business partners, and to the public.

From "if" to "how." The DSI Workgroup was originally chartered to explore *if* digital signatures should be adopted. When Executive Order 65 was released in late May, directing agencies to "take advantage of the benefits of digital signature technology to the fullest extent possible,[8]" the focus shifted to *how* digital signatures should be adopted. (See *Appendix A: Digital Signatures Initiative Deliverables* for more information on the Workgroup's charge in relation to Executive Orders 51 and 65.)

Goals of the report. The purpose of this report is twofold. First, the DSI Workgroup presents a record of its activities, findings, conclusions, recommendations, and a proposed plan of action for deploying an enterprise-wide digital signature solution. Second, the report aims to fuel the deployment effort with information, tools, and resources built on lessons learned. The report identifies critical issues, emerging technologies and policies, and open questions to guide the immediate deployment effort.

A demonstrated working solution of trust and confidence extensible to the Commonwealth public sector community, to business partners, and to the public.

An electronic version of the report and associated source documents is available in Adobe Portable Document Format (PDF) at http://www.sotech.state.va.us/cots/dsi.

[1] The National Council for Science and The Environment. "RL30435: Internet and E-Commerce Statistics: What They Mean and Where to Find Them on the Web." Congressional Research Service Issue Brief. February 17, 2000.

[2] Ibid.

[3] U.S. Department of Commerce. "The Emerging Digital Economy II: Electronic Commerce in the Digital Economy." Chapter 1. June 1999.

[4] Office of the Governor, Commonwealth of Virginia. "Executive Order 65 (00): Implementing Electronic Government in the Commonwealth of Virginia. May 24, 2000.

[5] U.S. Congress. "Electronic Signatures in Global and National Commerce Act." Senate Bill 761. January 24, 2000.

[6] American Bar Association, Information Security Committee, Section of Science & Technology. "Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce." Tutorial. August 1, 1996.

[7] Ibid.

[8] Office of the Governor, Commonwealth of Virginia. "Executive Order 65 (00): Implementing Electronic Government in the Commonwealth of Virginia." May 24, 2000.

[9] The National Council for Science and The Environment. "RL30435: Internet and E-Commerce Statistics: What They Mean and Where to Find Them on the Web." Congressional Research Service Issue Brief. February 17, 2000.

[10] U.S. Department of Commerce, National Telecommunications and Information Administration. "Falling Through the Net: Defining the Digital Divide." Table 1-3: Percentage of Households with Home Internet Access, by States. July 1999.

[11] Virginia Economic Development Partnership. "Why Virginia." www.yesvirginia.org

III. USER'S GUIDE

The report is organized into the following sections.

- ***Overview of Digital Signatures and PKI*** provides an introduction to digital signature and PKI terminology and concepts, and provides an overview of security in the electronic world, trust models, security requirements, management framework, and practical considerations. This section is intended for the digital signature novice and as a brush-up for readers with more experience. Those readers with a working knowledge of digital signatures and PKI may wish to advance to the next section.

- ***The Process*** highlights the methodology of the DSI Workgroup inquiry into digital signatures. This section provides an overview of research initiatives, including survey efforts, resources, and Education Day, as well as information on the robust pilot demonstration effort launched in Summer 2000.

- The ***Vision and Guiding Principles*** section articulates the DSI Workgroup's vision for digital signatures in the Commonwealth and the guiding principles adopted in conducting the inquiry.

- The major lessons learned and overarching conclusions of the DSI Workgroup are detailed in ***Findings and Conclusions***. Included in this section is information on trust, benefits of digital signatures, place of digital signatures in security architecture, complexity involved in deployment, systemic obstacles, process reengineering, synergies within the Commonwealth, and education and training.

- The ***Recommendations*** section articulates the recommended actions of the DSI Workgroup in the areas of open standards, interoperability mechanisms, legal counsel and liability, procurement of PKI products and services, governance, resources and funding, synergies, VOLT Early Adopters Program, education and training, and business process reengineering. This section also explores "horizon" issues—emerging applications and practices and evolving standards and technologies.

- ***Tools and Resources*** provides an overview of the solutions, tools, and resources cultivated by the DSI Workgroup and intended to inform the deployment effort.

- The ***Plan of Action*** is a time-phased workplan that illustrates roles and responsibilities for deploying digital signature technology in the Commonwealth of Virginia.

- The ***Appendices*** contain source documents and further information intended to fuel the implementation phase.

IV. Overview of Digital Signatures and PKI

Introduction. This section is designed for the digital signatures beginner and those wishing to brush up on terminology and concepts. The Overview is divided into two parts. The first part, *Introduction to Digital Signatures*, describes the concepts and functions behind digital signature technology. The second part, *Public Key Infrastructure*, highlights the definition and key components of a PKI. Consult *Appendix B: Glossary of Terms* for more information on terminology, and *Appendix C: Frequently Asked Questions* for more information on the DSI effort in the Commonwealth. For more information on digital signatures and PKI, visit http://www.sotech.state.va.us/cots/dsi/, and view two presentations by Tim Sigmon, Director of Advanced Technology at the University of Virginia.

Introduction to Digital Signatures

Trust and security. In conducting business in the physical world, we rely on established patterns of trust to guide our decisions. We have long-standing trust relationships with our retailers, employers, and government agencies. In the physical world, there is tangible evidence of identity—storefronts, nametags, state-issued identity cards, licenses, and other credentials—to provide reasonable assurance that the parties can be trusted; that they are who they say they are.

In the electronic world, we do not have the same trust cues to follow—we cannot “see” whom we are dealing with or know whether they are properly licensed or authorized to handle our transactions. The electronic world relies on a blend of technology and policy to establish trust relationships. One of the most powerful trust mechanisms is digital signature technology.

The electronic world relies on a blend of technology and policy to establish trust relationships.

Having the same legal ramifications as pen-and-ink (or “wet”) signatures, digital signatures are a string of numbers computed mathematically and attached electronically to a record to indicate the intent to sign the record. Because digital signatures employ public key cryptography, they are much more powerful than a wet signature. Digital signatures:

- Are tied to specific individuals and are legally binding;
- Ensure that data has not been tampered with since it was signed; and
- Prevent individuals from falsely repudiating transactions.

Public Key Cryptography

Cryptography has its roots in ancient history—Julius Caesar supposedly created one of the earliest cryptographic systems to communicate secret messages with his warriors. Until the invention of public key cryptography, people relied on symmetric cryptography. Caesar and his men, for example, used the same *key* to encrypt (scramble) and decrypt (unscramble) messages. One significant problem with this model is that—at some point—the key would have to be transported across geo-political boundaries and could thus be compromised. In addition, if Caesar corresponded with multiple warriors in many different parts of the empire, he may wish to have different codes for each to increase security. These men, in turn, would have to share keys to correspond among themselves. As the number of users increases, the number of keys to manage increases dramatically.

Key pairs. Public key cryptography—a recent invention—relies on two separate but interrelated keys and is known as asymmetric cryptography. Keys come in mathematically related pairs—a public key and a private key. The public key can be distributed publicly without compromising the integrity of the private key—the private key cannot be derived from the public key in any reasonable length of time. The private key must be kept secret and assigned to a single individual. Any data signed by the private key can *only* be unlocked or verified by the corresponding public key. Similarly, any encryption performed by the public key can only be decrypted by the corresponding private key. Because significantly fewer keys are involved in a network environment, key management is greatly simplified.

CRYPTOGRAPHY AND DIGITAL SIGNATURES

Digital signatures rely on public key cryptography to assure data integrity and support non-repudiation. In addition, public key cryptography can be used to provide confidentiality of the signed document. To understand how cryptography and digital signatures work in the electronic environment, the following example illustrates how to write and send a digitally signed check.

Security. Suppose you want to write a check, requesting your bank to pay a specific amount to a specific individual. When it comes time to send your check over insecure lines, you encounter several serious security problems:

- Someone could intercept or “sniff” your check and learn valuable information about you, such as your account number, contact information, and the specifics of your transaction, so you need confidentiality.
- Someone could falsely assume your identity and create similar, counterfeit checks, so the bank needs to verify that it was you who wrote the check.
- Someone could intercept your check and alter it, so the bank needs to know that the check has not been tampered with since you sent it.
- You could deny ever creating the check, so the bank needs non-repudiation.

Digital signatures rely on public key cryptography to provide security, assure data integrity and confidentiality, and support non-repudiation.

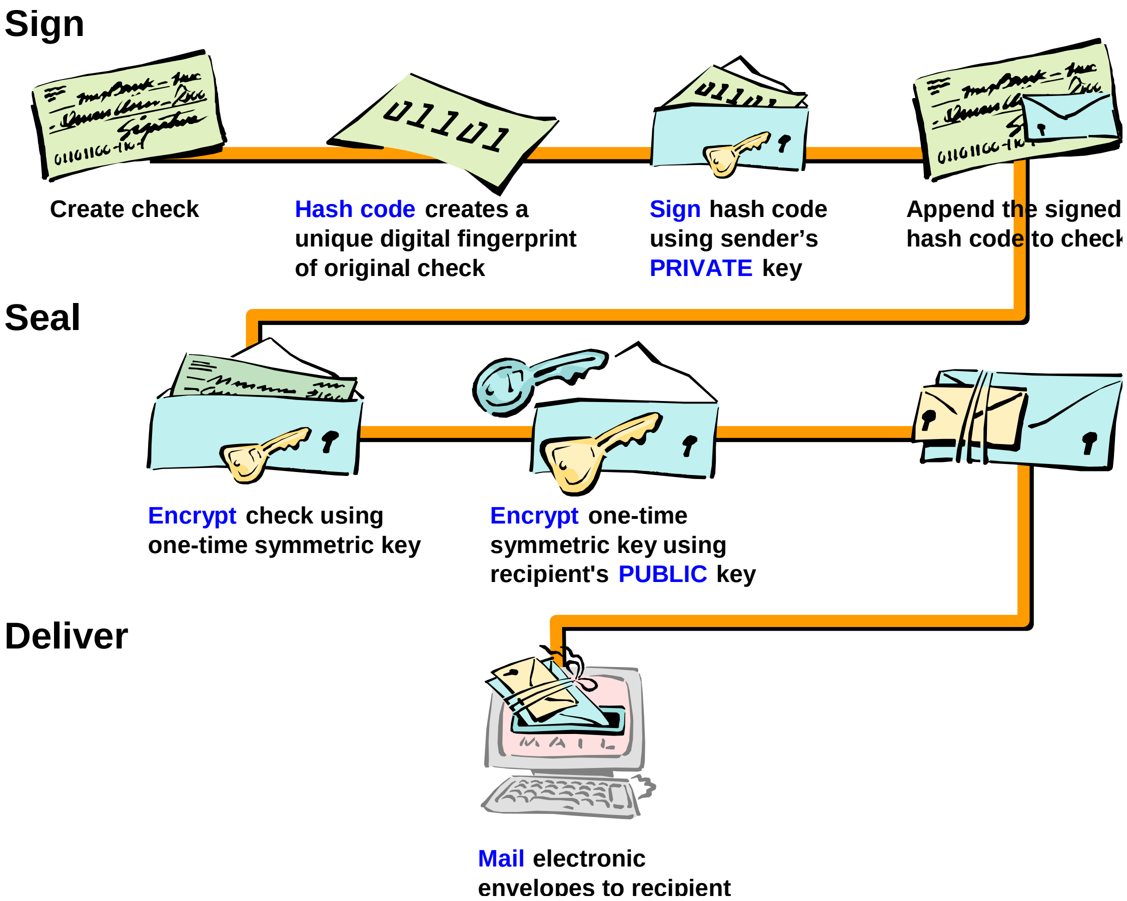
Digital signatures and encryption address these security problems. Most of the digital signature functions occur automatically in the background—the user follows a series of simple steps and questions, and is alerted if there is a breach in security. Here’s a behind-the-scenes look at how digital signatures works.

1. **Sign.** The first step to digitally signing the check is creating an “electronic fingerprint” or hash code of the check. If a single letter or digit of the message is changed, the hash code will change dramatically, alerting the recipient that the data may have been tampered with. Use your private signing key to encrypt the hash code of the check, and append the encrypted hash code to the check. This encrypted hash code is the digital signature.

2. **Seal.** To ensure the confidentiality of the check and ensure that the recipient is the only individual capable of opening your check, you should “seal” or encrypt the check. Public key cryptography can be used to encrypt documents, but it is unwieldy and slow, and is intended to encrypt small amounts of data. Symmetric key cryptography is designed to encrypt large quantities of data quickly. As discussed, symmetric keys have the problem that they have to be shared by some alternative means, so it is important to use a combination of public key and symmetric key cryptography to seal your check.

In this example, create a one-time symmetric key to encrypt the check. Once it has been encrypted, use the *recipient's* public key to encrypt the symmetric key. Why use the recipient's public key? The only key that can decrypt the data that was encrypted with the recipient's public key (e.g., the symmetric key) is the recipient's *private* key, to which only the recipient has access. If you used your private key to encrypt the symmetric key, your public key—which anyone can access through a directory service—can decrypt the symmetric key. By using the recipient's public key, you can be certain that the recipient is the only individual who can decrypt and read your check.

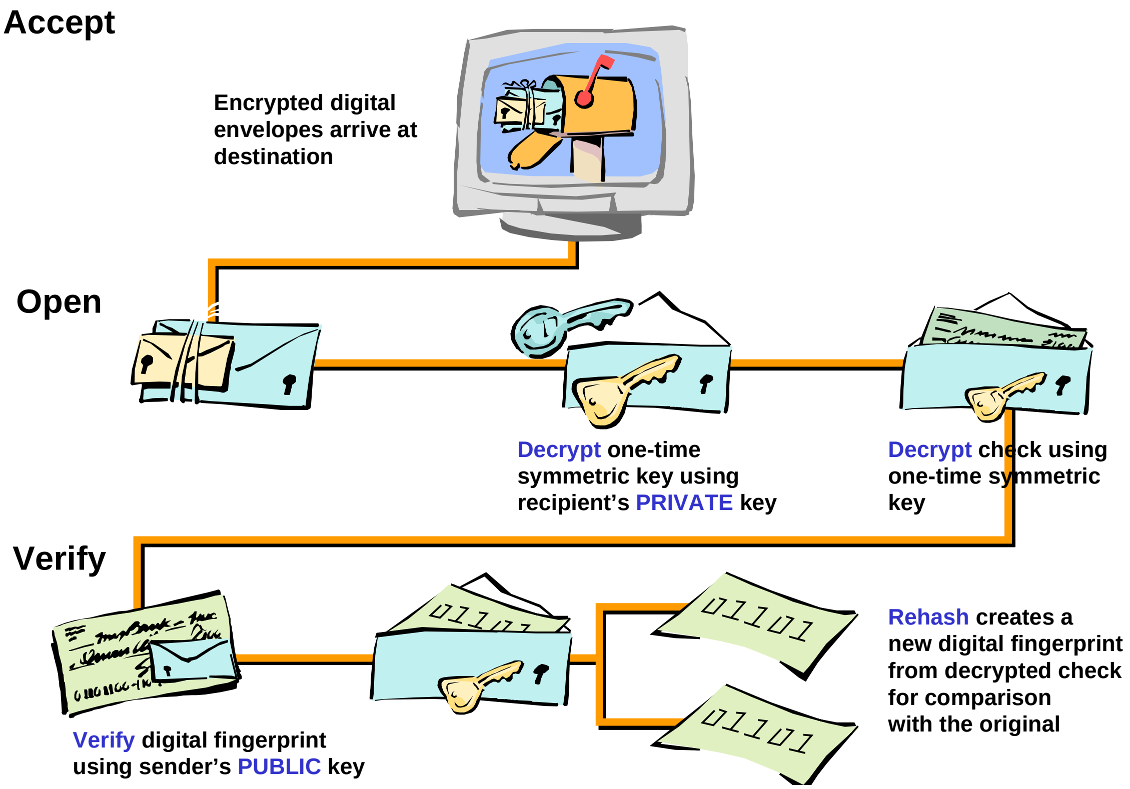
3. **Deliver.** Submit the encrypted hash code of the check, the encrypted check, and the protected encryption key to the recipient electronically.


Sign
Create check
Hash code creates a unique digital fingerprint of original check
Sign hash code using sender's PRIVATE key
Append the signed hash code to chec
Seal
Encrypt check using one-time symmetric key
Encrypt one-time symmetric key using recipient's PUBLIC key
Deliver
Mail electronic envelopes to recipient

4. **Accept.** The check and the accompanying materials arrive to the recipient.

5. **Open.** The recipient uses his or her private key to decrypt the one-time symmetric key. The recipient then decrypts the check.

6. **Verify.** To verify the identity of the sender, the recipient would use the sender's public key to decrypt the hash code of the check—the digital signature. A new hash code of the check is computed and compared to ensure the data was not altered prior to verification.


Accept
Encrypted digital envelopes arrive at destination
Open
Decrypt one-time symmetric key using recipient's PRIVATE key
Decrypt check using one-time symmetric key
Verify
Verify digital fingerprint using sender's PUBLIC key
01101
01101
Rehash creates a new digital fingerprint from decrypted check for comparison with the original

Public Key Infrastructure

PKI defined. A Public Key Infrastructure (PKI) is the framework of people and processes that manage trust and support electronic transactions. A PKI is a comprehensive system of policies and technology designed to provide digital signature services and public key cryptography.

Third-party trust. A PKI is necessary to foster trust, and revolves around the concept of third-party trust. In the physical world, for example, driver licenses are issued and "vouched for" by the Department of Motor Vehicles. When businesses or government employees authenticate your identity, they place trust in the people and processes behind the license. They trust the rigorous process DMV used to verify your identity, date of birth, and address—DMV is the trusted third party.

The same is true in the electronic world. Your digital certificate is like an identity card. For that certificate to hold weight, it must be issued by a trusted third party. In the check example above, the bank needs proof that you are who you say you are—that you are not falsely impersonating another account holder. A PKI provides the needed third-party trust, as well as functions related to all aspects of key and certificate issuance, management, and revocation.

A PKI provides the needed third-party trust, as well as functions related to all aspects of key and certificate issuance, management, and revocation.

The three major components of a PKI include:
1. Certification Authority (CA)
2. Registration Authority (RA)
3. PKI-Enabled Applications

Certification Authority (CA)

Certification authorities (CAs) are the trusted third parties that issue certificates and bind key pairs to a specific person or entity. The primary functions of a CA include:

- Issuing digital certificates;
- Revoking certificates;
- Providing status information on certificates it has issued; and
- Managing and storing certificates.[1]

Issuing digital certificates. Once an individual's identity has been verified, the CA creates and signs the digital certificate with its private signing key, called the root key. By signing each certificate, the CA is "vouching" for the validity of the certificate contents and binding the public key to a specific individual.

The processes and policies for issuing and managing certificates are articulated in the certificate policy (CP) and certification practice statement (CPS). A certificate policy is a broad statement of the general characteristics of the certificate, the user population, and specific purpose. Most CPs provide specific guidance in the following areas:

- Certificate contents;
- Identification and authentication methodologies;
- Certificate status protocol;
- Certificate management;

- Security audit procedures;
- Record retention, retrieval, and recovery;
- Physical, procedural, and personnel controls;
- Key generation and delivery;
- Private key protection;
- Key life cycle management; and
- Certificate revocation.[2]

One standard CP template and definitions of all provisions can be found at http://www.faqs.org/rfcs/rfc2527.html.

Certification Practice Statement. A certification practice statement (CPS) provides the operational details of how the certificate policies will be implemented. The CPS refers specifically to the daily operations of the CA and the detailed guidelines by which all certificate policies will be carried out.

Certificate contents. The industry standard for certificate structure is the International Standards Organization and International Telecommunications Union X.509v3 standard. According to X.509v3, certificates should contain information necessary to establish the identity of the user (such as name or unique identifier), identity of issuer (the CA), and basic certificate identifiers. Basic certificate identifiers include certificate version, serial number, the type of signature algorithm used by the CA, issuer name, validity period, public key information, and a pathway to the CA database containing status information.

Generating certificates. Janet wants to transact business with Jack using digital signature technology. To get her certificate, the first step is to generate the key pair. Key pairs can be generated by Janet's computer, or by the CA. The private key is safely delivered to Janet, and she sends the public key to the CA. Once the CA verifies Janet's identity, the CA generates Janet's digital certificate and signs it with the CA root key. Janet's public key is placed in a public directory so all PKI users can access it to verify her signature. The certificate is then loaded onto Janet's system.

Verifying signatures. Now that Janet has her digital certificate, she can transact business with Jack. She sends Jack a digitally signed purchase order for 3,000 widgets. Jack's software verifies the validity of Janet's certificate by obtaining the CA's public key and decrypting the CA's digital signature. Jack can also ensure that Janet's certificate has not expired or been revoked. One of the fields within her digital certificate is a pathway to a database owned by the CA containing certificate status information.

Certificate status. There are two types of systems for checking for revoked, suspended, and expired certificates. The older and less timely method is downloading a certificate revocation list (CRL), which is generated periodically by the CA. In a large PKI, the list could be lengthy and difficult to download. In addition, the information may not be up-to-date and accurate—Janet's certificate could have been revoked since the last CRL update.

The other method of checking certificate status is online certificate status protocol (OCSP). OCSP provides up-to-the-minute information, which could be of critical importance to a company handling millions of dollars of transactions in the span of an hour.

REGISTRATION AUTHORITY (RA)

Registration authorities (RAs) handle the initial requests for certificates. Before the CA issued Janet's certificate, Janet had to make a formal request for a certificate. Depending on the certificate policy and the level of assurance desired, the scope of the RA's work varies. For low assurance certificates, Janet may simply need to send an e-mail message or visit a web site. Certificates with higher assurance levels for transactions involving greater risk would require Janet to appear in person and provide documentation and proof of her identity.

The RA would receive Janet's request and handle the identity verification process for the CA, which is usually the most time-consuming aspect of certificate management. Once her identity was established and the registration process completed, the RA would send a request to the CA to generate Janet's certificate.

Large companies or government entities spread across geographical areas benefit most from registration authorities. A company with offices in San Francisco, London, and Paris, for example, could establish RAs in each location, even though the CA may be located in Virginia.

PKI-ENABLED APPLICATIONS

PKI-enabled applications include any program that is PKI-enabled. Most web browsers, including Netscape Navigator and Microsoft Internet Explorer, are PKI-enabled. Other off-the-shelf PKI-enabled software programs include e-mail clients (such as Microsoft Outlook and Netscape Messenger) and virtual private network (VPN) software and hardware. Extranets and VPNs use digital certificates to authenticate users outside of security firewalls.[3]

PKI CONSIDERATIONS

Interoperability. Even though Janet's telephone is made by a different manufacturer than Jack's telephone, the solid foundation of telecommunication standards and policies allow Janet and Jack to make and receive phone calls successfully. Similarly, on a network, the dozens or hundreds of proprietary components (hardware and software) are designed to meet industry standards so that they can be fully interoperable.

Because the international standards for PKI and digital signatures are in draft form and the technology is evolving rapidly, there are two primary interoperability issues that need to be considered. First, can Janet use Vendor A products and still communicate with Jack, who is using products from Vendor B (product interoperability)? Secondly, can Janet's CA trust Jack's CA if they operate in separate PKIs (trust domain interoperability)?

There are a number of interoperability mechanisms to address these problems. Some vendors offer plug-ins to convert data received from another vendor solution into useful forms. A bridge certification authority can map policies among multiple CAs and cross-certify root keys to expand the trust domain.

Private key security. Public key cryptography is a proven technology—no one has successfully “cracked” the code. As computers become more powerful and hackers more resourceful, the technology continues to evolve to deter technical security breaches. The weakness with any PKI, however, lies not in the technology but in the human element. There are two ways to compromise trust:

1. Lose control of an individual’s private signing key.
2. Compromise the integrity of the CA root key.

Integrity of private keys is the point of greatest risk in a PKI environment. Compromise of a private key’s complete association with the person or entity to which it was issued destroys that private key’s usefulness in any secure transactions. Thus, private key storage is a paramount concern.

Nearly all good current mechanisms of making a private key useable in more than one user environment involve hardware tokens. Web browsers are particularly vulnerable to attack, and exporting and importing certificates from one computer to another can be technically difficult and insecure. Other forms of security, such as biometrics and passwords and PINs can help protect the private key from misuse. One of the most difficult decisions facing those who wish to deploy PKI is deciding how to address the question of balance between cost and stringent measures to ensure the integrity of the private key.

Integrity of private keys is the point of greatest risk in a PKI environment.

Education and training. A critical component of an effective PKI implementation program will be education of the users. All users need to understand the importance of protecting their private keys. Sharing of one’s private key would be equivalent to giving someone “power of attorney” for an individual’s transactions. The second person would have all the access and abilities to conduct transactions of the key owner. The implications of sharing one’s private key are even more far-reaching than sharing passwords in the current environment because of the greater trust implied by the use of digital signatures—that trust enables a wider range of high-risk transactions using digital signature and thereby expands the vulnerability.

Encryption. Encryption is a method of protecting data by converting data into an unintelligible form that can only be returned to a readable state by using a special key or password to decrypt or decode it. Encryption is used to protect data while it is in transit and also when it is resident within a system or in storage.

Within the scope of this report, encryption is discussed relative to protection provided by its employment to ensure the integrity of the issuance, transmission, and storage of critical aspects of PKI-supported digital keys. In addition, encryption may also be used to prevent unauthorized alteration of a document once a digital signature has been affixed; especially while that document is being transmitted.

Information, files, and records resident within a system or while in storage may also be protected by using encryption. However, this usage of encryption is beyond the scope of this report. If an activity is currently using encryption, it is not intended that such protective measures currently in use, be replaced or altered due to the introduction of digital signatures. Encryption requirements used with digital signatures do not replace any requirements that are in effect for the use of encryption.

[1] Grant, G. L. *Understanding Digital Signatures: Establishing Trust Over the Internet and Other Networks.* New York: CommerceNet Press, McGraw Hill. 1998. Pg. 36.

[2] The Internet Society. "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (RFC2527). 1999. www.faqs.org/rfcs/rfc2527.html.

[3] Xcert International, Inc. "Building Trust on the Internet: A Practical Guide to Public Key Infrastructure." 1999.

V. The Process

DSI Workgroup Members and DSI Workgroup Contributors. The DSI Workgroup was comprised of representatives from five agencies, five localities, University of Virginia, and Virginia Information Providers Network (VIPNet). Organizations represented include:

- City of Charlottesville
- City of Norfolk
- County of Chesterfield
- County of Fairfax
- County of Wise
- Department of Game and Inland Fisheries
- Department of General Services
- Department of Information Technology
- Department of Motor Vehicles
- Department of Transportation
- University of Virginia
- VIPNet

Audit & Assurance Team. The DSI Workgroup established an Audit & Assurance Team—comprised of auditors and security professionals—to identify administrative obstacles, develop a digital signatures decision model, review standards, and develop an audit and control framework. Auditors representing the following organizations participated in weekly meetings between June and August 2000:

- Auditor of Public Accounts
- County of Chesterfield
- Department of Accounts
- Department of Game and Inland Fisheries
- Department of General Services
- Department of Information Technology
- Department of Medical Assistance Services
- Department of Motor Vehicles
- Department of State Internal Auditor
- Department of Taxation
- Department of Transportation
- Library of Virginia
- University of Virginia

Contributors. The DSI Workgroup also benefited from the extensive knowledge and experience of Commonwealth employees and contractors, the vendor community, other states, the Federal government, and the Government of Canada.

To get a jumpstart, the DSI Workgroup leveraged the best thinking and experiential learning of other states, the Federal government, and the private sector.

Methodology. To get a jumpstart, the DSI Workgroup leveraged the best thinking and experiential learning of other states, the Federal government, and the private sector. The DSI Workgroup first convened in December 1999, and conducted monthly business meetings to share information on best practices and methods for overcoming barriers and obstacles. (See *Appendix D: DSI Calendar of Events* for a complete accounting of the Workgroup's activities.)

RESEARCH

Resources. Throughout the duration of the Workgroup's inquiry into digital signatures, members visited pertinent web sites, reviewed journal and media articles, interviewed industry experts, and consulted with leaders of other PKI/digital signature deployments to stay abreast of developments and provide timely, insightful information for the Workgroup members. (See *Appendix E: Works Cited and Further Reading* for more information on selected publications and web sites.)

EDUCATION DAY

Held on March 15, 2000, at the University of Virginia, the Digital Signature Education Day was a focused workshop for the DSI pilot organizations. The purpose of the workshop was to educate Workgroup members and their pilot project staff members on digital signatures and deployment considerations, and to develop a blueprint plan of action for the pilot projects.

During the morning session, a number of agencies, localities, and vendors presented seminars on the following topics:

- Making the business case for digital signatures.
- Demystifying encryption and digital signatures.
- Department of Justice case study.
- Pilot project technical framework.
- Application integration and other operational topics.
- Auditability and management of records.

Presenters included representatives from:

- County of Fairfax
- Department of Information Technology
- Department of Motor Vehicles
- PEC Solutions, Inc.
- VIPNet

In the afternoon session, the organizational pilot teams broke out into facilitated work sessions to develop plans for making the pilot programs operational. As a result of Education Day, each pilot organization had a concrete plan of action for moving their pilot programs forward, and had the opportunity to learn best practices from industry experts and each other.

As a result of Education Day, each pilot organization had a concrete plan of action for moving their pilot programs forward....

STATE AUDIT SURVEY

In May 2000, the DSI Workgroup and DSI Audit & Assurance Team conducted a survey of all states purported to have digital signatures or PKIs in place, requests for proposals (RFPs) issued, or digital signature legislation enacted. The purpose of the survey was to gather information on audit efforts, criteria for when to use digital signatures, and standards and guidelines used. Representatives from 23 states were contacted, and asked the following questions:

- Describe the audit program that has been established for your PKI. Is it internally or externally conducted? What is the audit cycle? What are the objectives?
- Was there audit involvement in the development of your PKI? Is there an audit report that has been issued?
- For agencies and other organizations using digital signatures, do you have specific criteria for when digital signatures would/would not be used? What are these criteria and associated rationale? What are any operational or cost implications for the criteria that have been adopted? Were those guidelines established by statute, Executive Order, Administrative Authority, or some other means?
- Are there other standards and guidelines for use of digital signatures?

Findings. The Workgroup found that most states have had limited—if any—involvement in the investigation and development of the audit component of their PKI and digital signatures efforts. Several noted that the lack of involvement could be an impediment to deployment, and concurred that Virginia's approach to include auditor input was wise and beneficial.

In terms of decision model criteria, several states have determined uses for digital signatures in some form, but no state has firmly established a formal level of guidance in evaluating the usefulness of digital signatures. Other topics covered include:

- Access control mechanisms
- DMV as registration authority
- Single vs. multiple CAs
- State serving as central CA.

For more information, see *Appendix F: State Audit Survey Summary*.

Experiential Learning

Demonstration Effort

The Workgroup launched eleven digital signature with public key infrastructure (PKI) demonstrations in Summer 2000, and used the lessons learned from the demonstration effort to inform its findings and recommendations. The projects encompassed government to government (G2G) and government to business (G2B) initiatives. Four of the pilots involved communicating across layers of government—between a state agency and localities. All the pilots were tremendously successful tools of discovery. Pilot participants, partners, and projects include:

Department of Game and Inland Fisheries. The Department of Game and Inland Fisheries (DGIF) demonstrated agency-wide use of digital certificates for requests and approvals of purchases, travel vouchers, and law enforcement reporting forms. More than 600 certificates were issued to DGIF employees, who are located throughout the Commonwealth. DGIF plans to continue use of digital signatures, and intends to expand applications to include time accounting submissions, personnel forms, budget change requests, and, eventually, all other administrative paperwork.

All the pilots were tremendously successful tools of discovery.

Department of General Services. The Department of General Services (DGS) partnered with vendors in North Carolina and Massachusetts, the James River Correctional Center Purchasing Department, and the Division of Purchases & Supply (DPS) to test the use of digital signatures in the spot bid procurement process. The spot bid procurement process is initiated when an agency sends an Agency Purchase Request Form to DPS. The form must be signed (which commits agency funds) before the information can be entered into the tracking system. Once the information has been entered, it is forwarded to the purchasing supervisor responsible for that commodity. Following the solicitation process, the award notice and purchase orders are digitally signed. The award notice is posted on the DPS web site, and the digitally signed purchase order is sent to the winning vendor. As a result of the pilot, labor was reduced by 75 minutes per contract, and document travel time was cut significantly.

Department of Motor Vehicles. The Department of Motor Vehicles (DMV) participated in four pilot projects in the following areas:

- **Mobile Home Titling Fees** and **Additional Rental Sales Tax.** In partnership with Fairfax and Chesterfield Counties, DMV tested the exchange of data between local and state government. The demonstration objective was to evaluate the business impact of replacing manual signatures with digital signatures and to evaluate the integration of PKI into application software packages. It is likely that the pilots will move into a production environment.
- **Parking Ticket Information.** In partnership with the City of Charlottesville, DMV tested the use of digital signatures to exchange data between Charlottesville (local government) and DMV (state government). The demonstration objective was to evaluate the use of PKI encryption to determine what factors make encryption viable in a production environment.
- **Travel Authorization and Reimbursement.** The DMV Travel Authorization and Reimbursement Digital Signature Pilot was designed to educate the DMV user community on the benefits of digital signatures in an electronic, end-to-end PKI application. The application incorporated more than 25 vendor components and emerging technologies, such as extensible mark-up language (XML), smartcards, biometrics, web access control, and electronic workflow. Expected benefits include faster transaction time, electronic history of document path, earned trust of user community, faster reimbursement for DMV employees, and minimal or no paper trail. It is highly likely that this pilot will move to a production environment.

Department of Information Technology. The Department of Information Technology worked in partnership with DGS, Virginia Employment Commission, Department of Conservation and Recreation, DGIF, DMV, Chesterfield County, and the City of Norfolk to test the use of digital signatures in filing telecommunications requests. The digital signature provided the means by which to replace the current paper process with a web-enabled Telecommunications Service Request (TSR) form. The TSR form serves as a contract between the requestors and DIT to coordinate service from the phone company. Agencies and localities could submit and sign the TSR form and receive an order number in return. DIT plans to move the pilot into production.

Department of Transportation. The Virginia Department of Transportation (VDOT), in partnership with the Virginia Road and Transportation Builders Association and the Federal Highway Administration, demonstrated the use of digital signatures in electronic bidding. During two mock lettings, selected contractors submitted bids electronically to a system of servers designed to hold the data securely until the expiration of the bidding period. After the bid deadline, VDOT retrieved the data from the servers and processed it electronically, avoiding the current practice of keypunching. VDOT intends to move the pilot into production in late Fall 2000.

Virginia Information Providers Network. Working in partnership with DMV, the VIPNet Authority Board, Virginia Interactive, L.L.C., and the fiscal staff of DIT, VIPNet is launching a pilot to demonstrate the use of digital signatures to provide electronic authorization for interagency transfers. VIPNet, in its role as an information broker, handles commercial data transfers to authorized recipients and collects user fees. A small portion of the fee is retained by VIPNet to cover expenses, and the rest is transferred to the agency that owns the information. The policy governing the interagency funds transfer requires multiple signatures, and can take up to 14 business days to complete. VIPNet expects to cut the process time to seven days or fewer.

City of Norfolk. The City of Norfolk targeted the intranet personnel requisition system for its pilot demonstration. The personnel requisition system automates the submission and processing of personnel requisitions through a web interface. The system can be used to review the status of requisitions; record, track, and process requisitions; and generate reports and correspondence. Two steps in the hiring process require the production of a paper document due to the need for signatures. The document listing the candidates eligible for interviews must be signed by a Human Resource Team leader. Once a candidate has been selected for hiring, the signature of the City Manager or an Assistant City Manager is required to indicate approval for the hire. An electronic form was created that could be routed via e-mail for signature by the appropriate individuals. Due to communications and licensing agreement issues, the pilot was not fully launched. The anticipated benefits for the fully functioning pilot include time savings in the recruiting and hiring process, the reduction of paper in the workflow, and a fully automated process.

County of Wise. Wise County and the City of Norton, VA, process a large number of legal documents on a daily basis. Wise County chose to test the use of electronic signatures in the filing, searching, and retrieval of Deed of Trust documents remotely and electronically. Wise County and the City of Norton partnered with Big Stone Gap Housing Authority, the Law Office of Kern & Kern, a Notary Public, and Powell National Bank for the pilot. Wise County plans to move the pilot into production mode.

(See *Appendix G: DSI Demonstration Projects* for more information on the pilot programs, partners, objectives, and functions.)

Lessons learned. As a result of the pilot effort, a great deal of lessons learned, best practices, and hands-on experience with PKI and digital signatures was gained. Following is a summary of general lessons learned from the demonstration effort.

- Involve end users in all phases of planning, testing, and implementation.
- The learning curve is steep, especially with varied levels of computer literacy. Ongoing education and training is an essential component of a successful implementation. Vendors must be available extended hours to support implementation and maintenance of services.
- The relationship between clients and vendors is critical. Getting all participants to work together effectively is critical. Vendors and clients must clearly understand each other's requirements, capabilities, and constraints.
- Review vendor technical requirements well ahead of purchase in order to become aware of potential incompatibility issues.
- Top-level management should be involved from very beginning to understand the high-level of organizational and resource commitment required to implement and support PKI.
- Interdependence between users and systems must be understood by all.
- Applications integration is challenging. Setting up a test environment specific to the application is critical.
- New and evolving PKI technologies may be ahead of the current policy and legal framework.
- Digital signatures should only be implemented after all procedure, policy, and application options have been considered. Current business practices and policies may need to undergo a re-engineering effort to handle digital signature methodology while maintaining or increasing the level of controls and protection and to yield the greatest possible benefits.
- Using a forms package requires that each user has the package. Data extraction from forms is complex and requires field-level programming.
- By keeping authorization at the application level, rather than embedding authorization information in the certificates, modifications of authorizations can be accomplished without reissuing certificates.
- Consider the level of security and application requirements as critical factors in selecting key generation methods and storage media.
- Electronic forms should be accessible from a web-Server to provide a central point for access and a single point for version management. The form should be distributed through a browser, thus substantially reducing the overhead required to manage form releases and desktop updates.
- While E-form packages have developed substantial interoperability with PKI structures and to back-end databases, they are not interoperable with each other. A form developed with one vendor's software does not function in another vendor's environment.

Digital signatures should only be implemented after all procedure, policy, and application options have been considered.

THE BRIDGE

The University of Virginia conducted a limited and successful demonstration of a bridge certification authority (BCA). The BCA is modeled after the federal bridge project, and cross-certifies certification authorities (CAs) to promote interoperability and expand trust domains. In other words, the bridge cross-certifies the root keys of two CAs that agree their certificate policies and certification practice statements are acceptably similar. Thus, the holder of a certificate from one CA can conduct transactions with those holding similar certificates from any CA cross-certified through the bridge. The Workgroup learned that the bridge simplifies the cross-certification process by removing the administrative and technical burdens from the CA pool. The bridge is one mechanism by which to promote policy interoperability.

For more information on the Bridge demonstration, see *Appendix H: Commonwealth Bridge Certification Authority*.

VI. Vision and Guiding Principles

The DSI Workgroup supports the Governor's vision for The Digital Dominion—for improved, efficient operation of government and greater convenience and delivery of government services to citizens and businesses. The DSI Workgroup envisions creating an environment of trust, interoperability, and security for individuals and businesses conducting electronic transactions with the Commonwealth of Virginia.

> *The DSI Workgroup envisions creating an environment of trust, interoperability, and security for individuals and entities conducting electronic transactions with the Commonwealth of Virginia.*

Guiding principles. The DSI Workgroup built consensus around the following guiding principles, which provided a sound framework for the subsequent recommendations:

- *The power of attraction*. Create a voluntary, Commonwealth enterprise solution that will garner support and widespread use among agencies, institutions, and localities, not because it is compulsory, but because it is attractive, maximizes convenience for internal and external customers, optimizes ease of adoption and use, and makes the best business sense.
- *A solid foundation.* Our recommendations are framed to ensure integrity, flexibility, and maximum security balanced with the pace and scope of deployment. We want to build a solid foundation to position the Commonwealth to take advantage of the greatest gains in the rapidly-evolving technology marketplace.
- *Simplicity and flexibility.* To achieve early deployment and facilitate ease of adoption and use for agencies, institutions, and localities, our recommendations aim for the simplicity of the "cleanest," least complicated and most flexible technology and policy solutions.

> *Our recommendations are framed to ensure integrity, flexibility, and maximum security balanced with the pace and scope of deployment.*

VII. Findings and Conclusions

Introduction

Though the duration of the pilot demonstration effort was relatively brief, the DSI Workgroup gathered a substantial body of findings and a solid base of experience upon which to move forward. The following conclusions, lessons learned, and best practices are also derived from industry experts, research, and consultation with representatives from the federal government and other states in the process of deploying digital signature technology.

The Workgroup reached seven major conclusions in the course of the inquiry, in the following areas:

1. Importance of trust.
2. Best uses of digital signature technology.
3. Place in overall security architecture.
4. Complexity involved in deployment.
5. Systemic obstacles.
6. Value in business process reengineering.
7. Synergies with other Commonwealth initiatives and activities.

1. Trust is the linchpin of digital signature technology.

Trust. Trust is absolutely central to digital signatures, and digital signatures are essential to establishing trust in the electronic world. In the physical world, we rely on tangible evidence and clues to help us negotiate trust relationships. Most of us would not, for example, purchase a computer from an unmarked truck parked at the side of an interstate highway. How would we know the computer worked properly? That it wasn't stolen or poorly made? What legal recourse would we have if it's a hoax or if it malfunctions?

Trust is the linchpin of digital signature technology.

In the electronic world, these physical clues are gone. When I can't see you, can I trust that you are who you say you are? That I'm dealing with a legitimate party, not the truck on the side of the road? That my information won't be stolen or altered during transmission? That my data will get there at all? For more information on trust in the physical world vs. the electronic world, please see *Overview of Digital Signatures and PKI*.

Confidence. Confidence is the key to establishing trust in both the physical and electronic worlds. Users must have confidence in the security environment. Just as in the physical world, trust is half perception, half reality. If the stairs look rickety and may not support our weight, we will not make the climb. The same is true on the Internet. If the perception (or reality) is that safeguards are not in place, people will be hesitant to conduct business electronically. Thus, the highest level of assurance—which is afforded by digital signatures—is necessary to foster confidence and trust of potential users.

2. Digital signatures should be used for authentication, data integrity, and non-repudiation.

There are five major security requirements in the electronic environment:

- *Authentication* to verify and "prove" identity in order to avoid fraud;
- *Authorization* to allow someone with the proper credentials to perform transactions and prevent unauthorized persons from doing so;
- *Confidentiality and privacy* to ensure sensitive data is shared only with the individual(s) authorized to view it;
- *Data Integrity* to ensure the data has not been tampered with or altered during or after transmission; and
- *Non-Repudiation* to protect against someone falsely disavowing a transaction.

Though digital signatures can play an important role in confidentiality and privacy and in the authorization process, the Workgroup believes that digital signatures for the Commonwealth are best suited for the following purposes:

- *Authentication*. Digital signatures are tied to specific identities and can help prevent fraud.
- *Integrity of data*. Using a hashing function, digital signature technology computes and compares message digests to ensure data was not altered prior to signature verification.
- *Non-repudiation.* Because digital signatures are tied to specific individuals and are a legally accepted form of signature, they are legally binding.

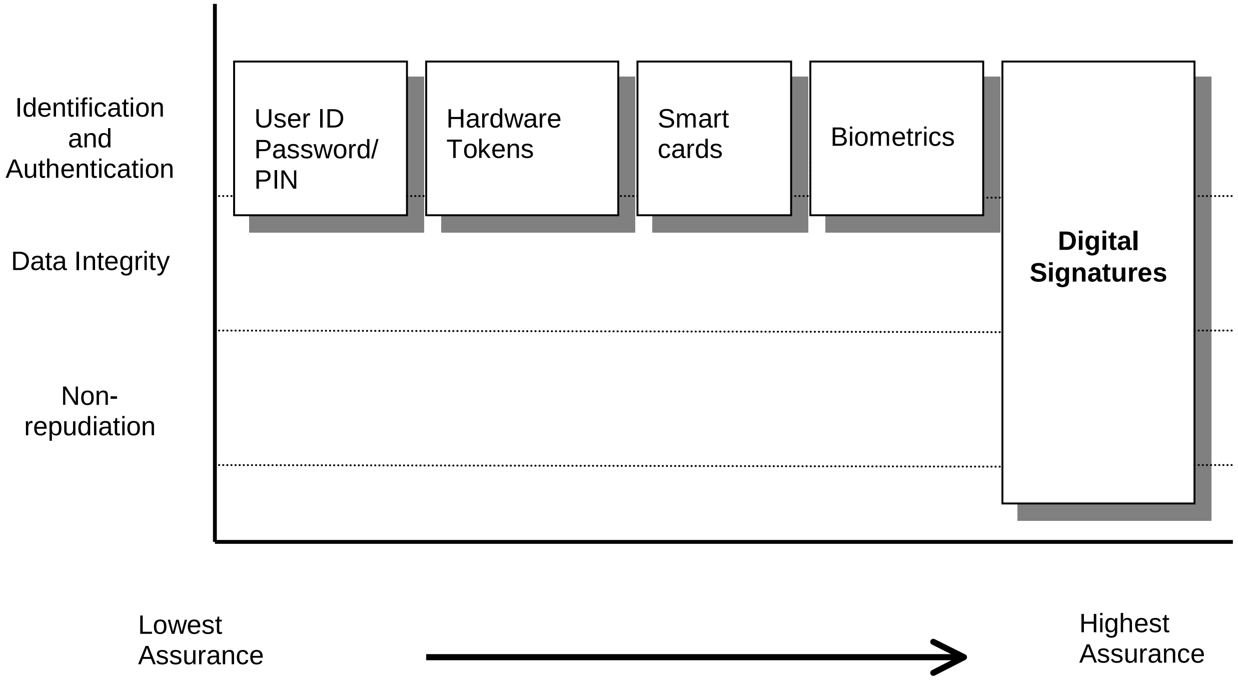
(For more information on making the business case for digital signatures in the Commonwealth, see *Appendix I: Digital Signatures Business Case*.)

3. Digital signature technology has a place in an overall security architecture.

A spectrum of options. Digital signatures are one form of electronic signing and one form of authentication. Other options—used singly or in combination—include double-clicks, passphrases and PINs, hardware tokens and smartcards, and biometrics. On the spectrum of electronic signatures, digital signatures are at the top. Digital signatures offer the highest level of assurance:

Digital signatures are but one piece of an overall security architecture.

SPECTRUM OF ELECTRONIC SIGNATURES



Appropriate functions. When issued using a stringent proof-of-identity registration model, digital signatures represent the highest level of assurance in verifying authentication, providing for integrity of data, and supporting non-repudiation. Because of the high assurance levels, digital signature technology is more complicated and costly to implement and use than other forms of electronic signatures, and may not be appropriate or practical for every application requiring a signature. For applications involving high risks and extremely sensitive data, and requiring a high level of assurance that the parties involved in the transactions are who they claim to be, digital signature solutions are unparalleled.

One tool in the toolkit. Digital signatures are not an either-or proposition—they are one tool for enabling secure transactions, and should exist in conjunction with other forms of security and electronic signatures. Similarly, digital signatures in and of themselves do not provide the basis for e-government. An absence of digital signature capability in the hierarchy of electronic signatures, however, can be an impediment to effective e-government.

Decision model. To assist Commonwealth agencies, institutions, and localities in determining when the use of digital signatures is appropriate, the Audit & Assurance Team has created the Digital Signatures Decision Model. *Appendix J: Digital Signatures Decision Model* contains a description and graphic depiction of the DS Decision Model, as well as a discussion of some additional decisions that must be made once it is determined that digital signature use for a transaction is appropriate.

4. Deploying digital signature technology is not a trivial exercise.

When the Privacy, Security and Access (PSA) workgroup report *Toward the Use of Digital Signatures in the Commonwealth of Virginia* was published in November 1999, several states seemed to be at the brink of deploying enterprise-wide PKI and digital signature solutions. A handful of states, including Illinois, New York, Texas, and Washington, had requests for proposals (RFPs) pending. The federal government—the public sector leader in PKI and digital signatures—was planning to expand its PKI services from 1,000 issued certificates to more than 72,000 issued certificates in 2000. Without immediate action, the PSA report concluded, the Commonwealth would be left in the PKI dust.

Barriers to implementation. Though all indicators pointed to rapid growth and use of digital signatures in 2000 and beyond, a number of barriers and inherent complexities have slowed progress in both the public and private sectors. These barriers, namely a lack of standards, interoperability issues, and legal and liability questions, are not new to PKI and digital signatures. Experts, however, predicted the rapidly evolving technology marketplace would push the resolution of these issues and open questions, opening the floodgates to mass adoption. That has not been the case.

Deploying digital signature technology is not a trivial exercise.

Legislative advances. Despite significant steps forward with recent federal (Electronic Signatures in Global and National Commerce Act) and state legislation (Virginia Uniform Electronic Transactions Act and Virginia Uniform Computer Information Transactions Act), deployments of digital signature technology continue to be limited in size and scope. Though the technology is maturing and continues to evolve, interoperability and standards issues remain unsettled and disparate. No state has moved into a full PKI production environment as predicted, though many continue to pursue pilot programs or measured, incremental enterprise solutions. Most states do not have an explicit statement of direction. Some states, such as Massachusetts, have backed away from implementing enterprise-wide digital signature solutions altogether.

Why? Despite claims or appearances to the contrary, our demonstration effort confirmed that digital signatures and PKI are far from being “plug and play” solutions. (See *Appendix G: DSI Demonstration Projects* for more information on the pilot demonstration effort and lessons learned.) Implementation involves:

- *Policy and business process decisions as well as technical expertise.* The participants in the demonstration effort learned that deploying digital signatures is approximately 60% policy and 40% technology. Participation across all levels of an organization is critical—business managers need to be involved as well as IT experts.
- *A significant investment of time, resources, and expertise.* Top level management needs to be involved from the very beginning to understand the extent of organizational and resource commitment required to implement and support digital signatures. End users need to be involved in all phases of planning, testing, and implementation.
- *A steep learning curve.* The technology behind PKI and digital signatures is complicated and abstract. The Workgroup members learned that deploying digital signatures involves multiple learning curves—the basic mechanics of the technology, the process of

application integration, the policies and business reasons behind processes and transactions, standards and interoperability issues, and cultural change.

- *Substantial process reengineering.* Moving a manual process to an electronic environment involves re-thinking the business process and the policies and guidelines that govern it. Participants found that extensive pre-planning was needed to address process reengineering and resource deployment.
- *Overcoming cultural, legislative, technical, and policy barriers.* Participants encountered a variety of obstacles, some of which were unique to the agency, institution, or locality, while others were widespread and systemic. Electronic voting—casting ballots in elections over the Internet—illustrates aptly the complexities involved. (See *Appendix K: Electronic Voter Registration and Electronic Voting* for more detailed information.)
- *Evolving standards.* Standards governing all aspects of digital signatures and PKI continue to evolve as the technology grows and matures. Multiple international standard-setting organizations are simultaneously developing standards to govern certificate functions and contents, registration and certification procedures, auditing and control functions, encryption, cross-certification, certificate revocation profiles, key recovery, and testing. The lack of established standards is a major barrier to adoption of digital signature technology, as the purpose of a standard is to “provide a common specification of syntax and semantics that can be used as a foundation for implementation.”
- *Interoperability issues.* There are two types of interoperability issues: product interoperability and policy interoperability. Despite the adoption of the few standards that exist, most notably the International Standardization Organization and International Telecommunications Union X.509 Recommendation for certificate structure and contents, most vendor products and solutions are not interoperable. A certificate from one vendor may not work immediately or easily in a different vendor environment. Assuming the technical interoperability issues can be worked out, there are considerable policy interoperability issues with which to grapple. Can User A trust User B’s certificate when it is issued outside of User A’s PKI environment? Did User A have to go through a similarly rigorous registration/authentication process to obtain the certificate? Are the security controls in environment A equally or more stringent than in environment B?
- *Open questions of liability.* Though the federal government and many state governments have passed legislation enabling electronic and digital signatures, there is no substantial body of case law. Differences in laws from state to state and internationally create uncertainty among businesses and governments attempting to conduct electronic commerce across geo-political boundaries.

Moving a manual process to an electronic environment involves re-thinking the business process and the policies and guidelines that govern it.

5. Digital signature and electronic government deployments are subject to systemic obstacles that can create a cycle of paralysis.

Transitioning to an e-government environment turns the “business as usual” (or “government as usual”) paradigm on its ear. Traditional methods of provisioning government and conducting government business—from budgeting to workflow to auditing—must be re-thought and reinvented. Though there is much pressure to “reinvent” government processes and transition services into the electronic environment, there are a number of systemic obstacles to change:

- *Infrastructure,* including the processes for budgeting and procuring hardware and software products and services. Technology has become as vital to the business function of government as utilities like telephones and running water. Yet, for the most part, technology needs are not treated as "cost of doing business." Waiting a year to get items approved in the budget process is nearly an eternity in Internet time. Virginia has established a Technology Infrastructure Fund to help jumpstart critical initiatives and cut the lag time significantly. The Commonwealth Seat Management Initiative also aims to shift investment strategies in technology infrastructure.
- *Cultural beliefs and practices,* such as resistance to change, distrust of technology, lack of awareness, and reliance on outmoded systems and practices like the traditional cost justification model vs. long-term strategic, customer-centered gains. Traditional cost models cannot quantify convenience and customer satisfaction—the primary goals of effective electronic government.
- *Funding,* to support systems change and cover substantial up-front costs and investments.
- *Staffing,* to provide horsepower for new development while continuing to maintain existing systems and services. The pilot demonstration proved that deploying PKI and digital signature technology requires highly trained and experienced staff.

Transitioning to an e-government environment turns the "business as usual" (or "government as usual") paradigm on its ear.

Many of these obstacles are inter-related and cyclical, often resulting in chicken-and-egg arguments like: "I don't have enough staff to put the needed infrastructure in place. We've done it this way for years and there are never any problems, and I can't get funding if there's no business need, and without funding I can't get staff or the equipment…." Effecting change in the fundamental way in which government conducts business requires breaking the cycle of systemic problems and gaining a critical mass of acceptance and support.

6. The greatest value of digital signatures lies in associated reengineering of business processes.

Automation provides convenience and cost savings, and digital signatures themselves provide trusted authentication and identification in the electronic environment. The greatest potential value may derive from the process of reengineering workflow and applications to create a customer-oriented electronic environment. Customer transactions that currently take days to go through a manual process will be redesigned to allow real-time, interactive transactions that can be completed in minutes.

The greatest value of digital signatures lies in associated reengineering of business processes and transition to best practices.

Raising standards. Digital signatures and automation present opportunities to raise standards for business processes, workflow, and security, and improve and redefine best practices. We want to put a working philosophy in place that we not replicate the security and accountability weaknesses and vulnerabilities often inherent in paper-based processes as we transition these processes into the electronic world. Several pilot participants found, for example, that digital signature technology provides a stronger audit trail and added security in terms of data integrity and authentication. The DMV travel reimbursement pilot, for example, 'locked' travel expense data in the form once the traveler signed it, so that it could not be altered. In the paper world, it is nearly impossible to determine whether data was changed, and, if so, when.

7. Digital signatures are connected to and can advance other Commonwealth initiatives and activities toward a seamless implementation of electronic government.

The progress of the DSI Workgroup interrelates with Executive Orders 51 and 65 and with other initiatives spearheaded by COTS, the Secretary of Technology, and his reporting agencies. In particular, the work of the following groups or initiatives provides specific opportunities to create synergies:

a) COTS Privacy, Security and Access (PSA) Workgroup. The PSA Workgroup is focusing on:

- Enhancing the awareness of and confidence in the privacy and security tools available on the web and dispelling misinformation that may exist on the topic among agencies and the public.
- Clarifying the Commonwealth's current legal and policy framework within which decisions must be made.
- Identifying and recommending best practices, guidelines, or architectures for agency adoption.
- Developing a resource directory for agency use.

b) COTS Enterprise Architecture/Security Workgroup. The primary goal of the Commonwealth of Virginia Enterprise Architecture Initiative is to establish an enterprise architecture process that is focused on building and maintaining an enterprise-wide technical architecture. The technical architecture should best enable the priority business activities of state government and facilitate the adaptation of technology to the changing business-driven needs of the Commonwealth.

The DSI Workgroup has concluded that digital signatures rely on the framework of an enterprise-wide security architecture. Without a firm foundation of security, digital signatures cannot be employed properly. In terms of the physical world, deploying digital signatures without paying heed to the underlying security infrastructure is akin to building a castle and a moat but leaving the drawbridge down. Digital signature technology is only as strong as the existing security infrastructure, and all vulnerabilities must be addressed.

c) Department of Technology Planning. The Department of Technology Planning (DTP) promotes the effective and efficient development and use of technology that serves the needs of state government and the citizens of the Commonwealth. DTP's primary area of responsibility includes information technology as well as the full spectrum of technology solutions and innovations. Current initiatives include the Land Records Management Task Force, the Virginia Geographic Information Network, the Office of Innovative Technology, and the Enterprise Architecture Initiative.

Digital signatures and automation present opportunities to raise standards for business processes, workflow, and security, and improve and redefine best practices.

d) **Executive Order 51 E-forms and digital signatures.** Executive Order 51 requires all executive branch agencies to provide all forms needed by citizens via the Internet and supply DTP with plans for transitioning paper-based processes to an electronic environment. According to the Order, "Agencies and institutions shall follow the

Secretary of Technology's guidance in incorporating into their proposed plans for web-enabled government the use of electronic signature technology for both internal and external transactions.[1]" The DSI Workgroup has conducted a review of agency and institution EO 51 plans. (See *Appendix L: Executive Order 51 Review* for more information.)

e) **Executive Order 65 Administrative Applications.** Executive Order 65 calls for executive branch agencies to implement electronic government and created the Electronic Government Implementation Division (eGov) to help agencies and institutions move services to the Internet. The Order also addresses specific initiatives, including electronic procurement, administrative applications, digital signatures, privacy and security, seat management, and digital opportunities. The DSI Workgroup recognizes an important linking opportunity to Administrative Applications:

> "Web-based technology can be applied to a wide range of administrative processes within state government, used by virtually every agency, to make them more efficient. These processes include, but are not limited to, employee benefits administration, leave reporting and accounting, travel planning and booking, motor pool reservations, and expense reporting.[2]"

…digital signatures rely on the framework of an enterprise-wide security architecture.

f) **COTS Seat Management Program.** The COTS Seat Management Workgroup was designated in November 1998 to discuss alternatives to state and local government purchase of PC desktop technology. The concept, called seat management, is a performance-based contractual agreement that provides for total PC desktop management to become a utility. The Workgroup has researched the Internet, interviewed federal, state, and local government officials, and invited vendors to present on the issue of seat management. As a result of the Workgroup's recommendations, the Commonwealth of Virginia is in the process of negotiating a statewide seat management contract, which will be available in the fall of 2000. Seat management provides for a full range of computer services at each employee's desk or "seat." Virginia is the national leader in developing a statewide seat management contract.[3]

g) **Commonwealth Portal Strategy.** An enterprise portal strategy provides citizens, businesses, and employees with a single point of access to government information and services that is integrated, customizable, and personalized. In other words, users can control the look and feel of the site, receive information and reminders specific to their needs and interests, and locate services and forms easily across local and state government lines and across agencies. Digital signatures will be one component of the portal architecture. This would best be determined prior to building the digital signature framework rather than having to retrofit.

h) **Commonwealth Kiosks.** If the Commonwealth deploys kiosks, they need to be architected to anticipate digital signatures, most probably in the form of smartcards. To avoid unnecessary obstacles and incurring additional expense, now is the best time to decide how to incorporate digital signatures into the architecture.

SUMMARY CONCLUSION

Relying on the guiding principles and findings and conclusions articulated by the DSI Workgroup, the Commonwealth should deploy digital signature and PKI technology strategically. Recognizing the legal, policy, technical, operational, cultural barriers; uncertainties related to applied case law; and the continued evolution of associated standards and products, the Commonwealth should move forward strategically to build momentum and the infrastructure that would support a full-scale PKI production environment.

To that end, the DSI Workgroup believes the Commonwealth should adopt an enterprise solution of trust—a solution that offers a wide array of digital signature and PKI products, provides flexibility and simplicity, and promotes interoperability. By providing an enterprise solution, agencies, institutions, and localities do not have to invest significant time and resources in developing internal digital signature expertise and security infrastructure. A standards-based enterprise solution promotes interoperability, while allowing agencies, institutions, and localities to customize and adapt the technology to meet their business needs. Similarly, by articulating those standards, entities that choose to develop their own infrastructures will know the criteria to aim for.

The Commonwealth should adopt an enterprise solution of trust—a solution that offers a wide array of digital signature and PKI products, provides flexibility and simplicity, and promotes interoperability.

[1] Office of the Governor, Commonwealth of Virginia. “Executive Order 51 (99): Implementing Certain Recommendations by the Governor’s Commission on Information Technology.” July 23, 1999.

[2] Office of the Governor, Commonwealth of Virginia. “Executive Order 65 (00): Implementing Electronic Government in the Commonwealth of Virginia.” May 24, 2000.

[3] COTS Seat Management Workgroup. “Seat Management for the Commonwealth of Virginia.” September 1999.

VIII. Recommendations

The Workgroup has crafted numerous recommendations to support implementation of digital signatures. Designed to ensure maximum flexibility and simplicity, the recommendations can be grouped into the following ten areas:

1. Virginia On-Line Transaction (VOLT) Certificates.
2. Interoperability mechanisms.
3. Legal counsel.
4. Procurement(s).
5. Governance and oversight.
6. Resources and support.
7. Synergistic approach.
8. VOLT Early Adopters Program.
9. Education and training.
10. Horizon issues.

1. Issue Virginia On-Line Transaction (VOLT) Certificates.

To ensure interoperability, portability, and simplicity, the Workgroup recommends issuing VOLT Certificates that adopt open standards, provide high levels of assurance, and would be used for identity only. Individuals could use VOLT Certificates with participating agencies, institutions, and localities, thereby lifting substantial key management burdens from the user. Open standards are vendor-neutral, and promote interoperability among multiple CAs. By adopting a suite of open standards as the default, the Commonwealth will ease the burdens of decision-making for all agencies, institutions, and localities implementing digital signatures. (For more information on open standards, see *Appendix M: VOLT Open Standards Proposal*.)

To ensure interoperability, portability, and simplicity, the Workgroup recommends issuing VOLT Certificates that adopt open standards, provide high levels of assurance, and would be used for identity only.

Open standards. The Workgroup recommends that the open standards include, among others that will be developed and finalized in subsequent phases of development:

- Digital certificate structure (X.509 v3)
- Certificate contents (identity only—authorization to be handled by applications)
- Types of certificates (high assurance level; certificates for business representatives with high levels of affiliation verification; certificates for relying parties)
- Registration processes (specific to each type of certificate)
- Various operations related to certificate management and issuance (including certificate revocation lists (CRLs), recovery mechanisms, etc.)
- Document retention and retrieval (within state-mandated schedules).
- Audit and control standards, as articulated by the Audit & Assurance Team. (See *Appendix N: Internal Control and Auditing Standards* for more information.)

Identity only. The Workgroup recommends that VOLT Certificates should be as “clean” as possible, including identification information only. The structure of the VOLT Certificate will follow an internationally accepted structure to provide an identity certificate that can be used for multiple applications.

High assurance level. In the initial stages of deployment, the Workgroup recommends issuing high assurance certificates only to ensure users understand the need to maintain absolute control over their private signing keys. Digital signature technology is designed to provide maximum security for highly sensitive transactions that involve some level of risk. The Workgroup believes that other forms of electronic signature provide adequate protection for other transactions. Though many CAs issue low assurance certificates (known as “drive-by certs”) that require no in-person authentication or proof of identity, the Workgroup recommends instituting a Commonwealth PIN.

Commonwealth PIN. The Commonwealth PIN could be used by individuals across agencies, rather than having a separate user ID and PIN for each government entity. The Commonwealth PIN should be based on a universal unique identifier that would not be tied to a sensitive piece of identity. Social security numbers, for example, have meaning in many contexts and would not be a good candidate for the Commonwealth PIN.

2. Develop and deploy interoperability mechanisms.

To foster a multi-layered, multiple-vendor environment, the Commonwealth must explore and deploy interoperability mechanisms (such as bridges) to expand the domain of trust. The University of Virginia demonstrated the efficacy of the Bridge Certification Architecture to perform cross-certifications among multiple CAs. Cross certification allows relying parties to enjoy the benefits of multiple trust hierarchies without having to exist within that hierarchy or manage an unwieldy number of trust relationships. For more information, see *Appendix H: Commonwealth Bridge Certification Authority*.

High assurance certificates issued by other governmental entities—such as the U.S. Department of Defense—could be reviewed and accepted by the VOLT Governance Team to be used alongside the VOLT Certificate. The Workgroup also recommends that the Commonwealth monitor emerging guidelines and standards at the international and national levels.

3. Involve legal counsel that understands the technology to advise on issues of liability and legality and assists to advance the Administration’s goals for The Digital Dominion.

The Workgroup recommends the Office of the Attorney General consider creating, administratively or through legislation, a Division of Electronic Government to provide dedicated advice and assistance to all agencies and institutions of the Commonwealth. This new division in the Office of the Attorney General is analogous to the Division of Consumer Counsel (sec. 2.1-133.1) and the Division of Debt Collection (sec. 2.1-133.4). The purpose of establishing a dedicated legal division is to provide the technological/legal expertise necessary to guide the Commonwealth’s agencies and institutions through the cutting edge issues that characterize e-government at a pace that supports a leadership position for the Commonwealth.

New legislation. During the past year, both the Federal and State governments have passed significant legislation related to the conduct of business electronically, including the use of electronic signatures. On April 9, 2000, Governor Gilmore signed one of the nation's first Uniform Electronic Transactions Act (UETA). On June 30, President Clinton signed the E-Sign Law.

Overlap. It is important to note there is significant overlap between the federal E-Sign Law and the Commonwealth's UETA. Though the Federal E-Sign Law contains provisions for preemption of state laws, there are caveats to the preemption that must be evaluated, such as a caveat regarding non-uniform provisions. A number of important exclusions to the E-Sign Law exist, which are not paralleled in the UETA, such as cancellation or termination of utilities. For more information on the overlap with the two pieces of legislation, see *Appendix O: Comparison of Electronic Signature Legislation*.)

Lack of precedents. It is equally important to note the legislation is new and few precedents have been set to guide the formation of e-government policies and best practices within the Commonwealth. The interpretation of these legislative efforts within the courts will be a deciding factor in their validity. Further, the exponential growth of technology and related evolving business practices have placed legislation at ever level—global, federal, state, and local—in a reactionary mode.

It is of paramount importance to the success of digital signatures, specifically, and e-government, in general, to have expert legal advice in formulating optimal policies, procedures, and practices. For more information on the legislative environment, see *Appendix P: Legislative Environment*.

4. **The Department of Information Technology, with direction from the Secretary of Technology and the support of the Electronic Government Implementation Division (eGov), should develop and manage the procurement of digital signature-related products and services for use by agencies, institutions, and localities.**

Out-sourced solution. The Workgroup recommends out-sourcing certification authority (CA) functions to leverage industry expertise and hasten deployment. Though the demonstration effort boosted significantly the level of experience and expertise, the Commonwealth does not have the infrastructure or capacity at this time to provide an in-sourced solution and maintain the momentum generated to date.

Multiple CAs. To ensure a multi-layered environment with multiple CAs, the Workgroup recommends contracting with an enterprise PKI services coordinator that will work with multiple vendor products and solutions and provide technical assistance. The Workgroup envisions a "one-stop shop" approach to the provision of PKI and digital signature services. An agency, institution, or locality interested in deploying digital signature technology can go to a single source to choose from an array of solutions and receive the necessary technical assistance for planning, deployment, and maintenance. In this trust model, multiple CAs can—and will—coexist,

In this trust model, multiple CAs can—and will—coexist, relying on the VOLT open standards and interoperability mechanisms.

relying on the VOLT open standards and interoperability mechanisms. Agencies, institutions, and localities can make informed decisions and implement solutions without starting at the very bottom of a steep learning curve.

RFP components. The Workgroup recommends that the RFP(s) address provisioning the following key areas:

- CA products and services
- Interoperability mechanisms (such as a bridge CA)
- Commonwealth PIN management
- Application and platform integration products and services
- Education and training
- Marketing and promotion
- Document retention and recovery mechanisms

The Workgroup has collected a number of source documents, including sample RFPs from Washington state and Utah, to inform the development of the RFP for the Commonwealth. (See *Appendix Q: RFP Resources* for more information.)

5. Reconfigure the DSI Workgroup and establish the Digital Signature Deployment Workgroup to provide implementation oversight.

DSI Workgroup membership was limited to two members from each Commonwealth organization participating in the demonstration pilots. The Workgroup should be reconfigured to match the new proposed deployment effort, and open to new members. The Workgroup recommends designating the following teams to assist in the deployment effort (see *Appendix R: Proposed Digital Signatures Deployment Workgroup Organization* for more information.)

The Workgroup should be reconfigured to match the new proposed deployment effort, and open to new members.

- **VOLT Governance Team.** The VOLT Governance Team, a body of COTS assisted by eGov, would recommend policies to the Secretary of Technology for governing the operation of digital signature implementation. Specifically, the VOLT Governance Team could be charged with:
  - Developing a concept of operations to help guide the procurement effort and serve as the basis for the certificate policy and certification practice statement(s) (CP/CPS). (See *Appendix S: Concept of Operations Outline* for more information.)
  - Developing and recommending VOLT certification policy and practice statements, operating rules, and applications processes.
  - Coordinating review and resolution of legal, policy, technical, and business issues.
  - Set standards for achieving interoperability.
  - Overseeing the VOLT Early Adopter's Program, including identifying and recruiting candidates. (See *Appendix T: VOLT Early Adopters Program Concept Paper* for more information.)
  - Crafting the CP and CPS that will govern all aspects of CA and RA functions and processes
  - Providing oversight of the central PKI services coordinator, including policy and practice decisions.

  (For more information, see *Appendix U: Proposed VOLT Governance*

Charter.)

- **Procurement Team.** The Procurement Team would be responsible for overseeing the RFP process for securing a central PKI services coordinator and application integration services. The Procurement Team could be charged with:
  - Coordinating efforts with the Secretary of Technology, the Department of Information Technology, Department of Technology Planning, the Electronic Government Implementation Division, and the VOLT Governance Team to develop a procurement strategy.
  - Developing the RFP(s) for needed digital signature products and services.

- ***Audit & Assurance Team.*** The Audit & Assurance team will continue to play a very active and important role in the implementation effort, including informing the procurement effort on security and control standards and helping to resolve and remove operational obstacles tied to auditing and finance. Many of the audit and assurance issues will link closely to legal and liability issues.

- **Emerging Technology Team.** The Emerging Technology Team would monitor emerging technical and standards trends for applicability to the Commonwealth's digital signature initiative specifically and e-government generally. The Emerging Technology Team could be charged with:
  - Monitoring emerging standards, tools, and technologies for opportunities for linking and leverage in the Commonwealth.
  - Recommending strategies for optimizing emerging technologies and trends to promote digital signature deployment.
  - Sharing information on best practices and emerging trends with COTS and to inform other Commonwealth workgroups and initiatives.

- **Business Connections Team.** The Business Connections Team would explore national and international models, programs, and initiatives that may provide opportunities for mutually beneficial partnerships with other organizations.

- **Education and Promotion Team.** The Education and Promotion Team will provide education and training to build awareness about and familiarity with digital signatures and perform outreach to agencies, institutions, and localities to increase involvement and participation.

6. Provide resources and support for agency, institution, and local government adoption of PKI and digital signatures.

The Workgroup recommends providing seed money, resources, and other incentives to promote use of digital signature technology. The Secretary of Technology should secure a funding source and provide for project management. Though use of digital signatures will result in cost savings over time, the startup costs can be significant.

The Workgroup recommends providing seed money, resources, and other incentives to promote use of digital signature technology.

The Workgroup developed a cost model that identifies the basic cost elements for implementing digital signatures:

- Hardware and software acquisition
- Consulting, installation, configuration, integration, and testing services
- Staffing and training
- Facilities
- Ongoing maintenance

Alternative pricing strategies for cost components have been identified. (For more information on costs, see *Appendix V: Digital Signatures Cost Model*.)

7. Connect with Commonwealth initiatives and activities to promote a unified, synergistic approach to electronic government implementation.

Executive Order 51. The Workgroup recommends building on opportunities from Executive Orders 51 and 65 to boost electronic government and deploy electronic and digital signatures. Agencies and institutions should follow the Secretary of Technology's guidance per EO 51 in incorporating electronic and digital signatures into their applications.

EO 51 also required all Executive Branch agencies and institutions to develop plans for delivering current and expanded services through the Internet. To complete this directive, DTP instructed applicable agencies and institutions to report their plans for web-enablement in terms of the following five tiers:

Tier One—No forms on web site
Tier Two—MS Word (or other off-the-shelf software used for forms)
Tier Three—PDF formats for forms
Tier Four—HTML (interactive) formats for forms
Tier Five—HTML formats with digital/electronic signature.

Tier two is the minimum to achieve compliance with the December 31, 2000, web-enablement requirement.

Our review. The DSI Workgroup commissioned a review of EO 51 planning documents to learn which agencies and institutions had plans for Tier Five applications. The resulting recommendations include:

- Distribute COTS Digital Signature Initiative final report to all agency heads and authors of the EO 51 documentation to supplement their planning efforts.
- Provide a targeted education program to provide a digital signature primer.
- Consider involving the Center for Innovative Technology as a participant in the deployment process, given their mission and the scope of projects currently in place.

Executive Order 65. The Workgroup recommends considering administrative applications, as defined in EO 65, as candidates for digital signature technology. These processes—used by virtually every agency in the Commonwealth—include:

- Employee benefits administration
- Leave reporting and accounting
- Travel planning and booking

- Travel reimbursement
- Motor pool reservations
- Expense reporting

EO 65 calls for developing web-based solutions for these applications that can be adopted by agencies, institutions, and localities and customized to meet their business needs.

8. **Launch the VOLT Early Adopters Program for agencies, institutions, and localities that are willing and capable to deploy digital signatures in a production environment.**

Modeled after the Washington Early Adopters and Illinois' Seed Certs programs, the VOLT Early Adopters Program will demonstrate success in G2G, G2B, and G2C applications, boost confidence, and build momentum for future deployments. According to the *VOLT Early Adopters Program Concept Paper (Appendix T)*, candidates for the program should have some of the following characteristics:

- A sound security infrastructure in place
- Human resources to support the new technology
- Interaction with a significant government or education community
- Interaction with citizens and external partners
- Funding to support additional costs
- Processes which will benefit from the application of the technology
- Applications that can be logically enabled to support interoperability
- Administrative applications from EO 65.

The outcome of the initiative will be a solid infrastructure that will support the use of digital signatures for electronic government applications in the Commonwealth of Virginia. The Workgroup recommends the following activities to ensure success:

- Ensure program is data driven with user feedback.
- Partner with agencies, institutions, local governments, the business community, and vendors.
- Development of reusable application mechanisms for use by every level of government.
- Coordinate efforts with other Commonwealth workgroups and initiatives.
- Work with the agencies of the Electronic Government Implementation Division to integrate resources and identify cross-agency applications.

9. **Provide education and training to build awareness about and familiarity with digital signature technology and its benefits and implementation decision factors.**

Conduct an education and awareness campaign targeted to Virginia employees in agencies, institutions, and localities; legislators; and segments of the business and citizen populations.

As stated in EO 65, the Electronic Government Implementation Division should educate agency leaders interested in or considering adopting digital signature technology.

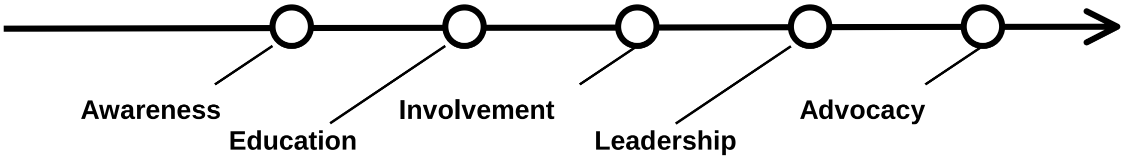
Provide education and training to build awareness about and familiarity with digital signature technology and its benefits….

All digital signature users should receive security awareness training for private key protection before high-assurance key pairs are issued. All digital signature users should formally acknowledge their responsibilities for protecting their private key before access to any system utilizing the high-assurance key is granted.

Mobilizing leadership. For the Digital Signatures Initiative to be successful and fully take hold in the Commonwealth, we need to mobilize leadership and cultivate a group of advocates for the technology. Cultivating leadership requires the following steps:

- *Awareness*—Introducing the concepts of and making the case for digital signatures.
- *Education*—Providing hands-on instruction in how the technology works and how it can be best applied within agencies, institutions, and localities.
- *Involvement*—Encouraging participation and adoption of digital signatures.
- *Leadership*—Once individuals have had positive experiences with the technology and an understanding of how it works, they can provide leadership within their organizations to deploy digital signatures across a multitude of applications.
- *Advocacy*—Leaders become advocates when they champion the digital signature cause outside of their agencies and organizations, persuading others to investigate and adopt the technology.

Leadership Mobilization Continuum



10. Leverage the learning and expertise of others, and monitor emerging technologies and security solutions for applicability to the Commonwealth.

Because the environment continues to evolve rapidly and operates in a larger context than a single entity, region, state, or country, there are significant opportunities for linking, leveraging, and leadership on the horizon. The Emerging Technologies and Business Connections Teams should monitor emerging models, policies, and practices and evolving standards and technologies:

EMERGING MODELS, POLICIES, AND PRACTICES

- **Health Insurance Portability and Accountability Act (HIPAA) of 1996.** Acting under pressure from consumer and patient protection groups, Congress moved to ensure the security of health-related information transmitted electronically with the passage of HIPAA. HIPAA affects health care providers, health plans and health care clearing houses, and directs the U.S. Department of Health and Human Services to develop information security standards to protect individual health information. It will require all U.S. healthcare organizations that transmit or store electronic messages or records pertaining to individual patients to prevent unauthorized use or disclosure of such information, while also ensuring easy access for authorized users and approved purposes.

  Virginia agencies involved in healthcare and their private partner organizations must establish clear administrative procedures to ensure the integrity, confidentiality, and availability of patient information. In addition, they must employ technical security services to ensure the physical safeguards to control access to patient information and provide for audit trails that record all access to patient information. These organizations may elect to adopt digital signature technology to ensure message integrity, authenticate users, and support non-repudiation. (For more information on HIPAA and how it affects Virginia, see *Appendix W: Health Insurance Portability and Accountability Act*.)

- **Electronic notaries.** There is a great deal of interest nationally and within the Commonwealth in electronic notaries and in defining new roles for notaries as important components of a high-assurance digital signature registration process. Several states, including Arizona, Nevada, and Minnesota have passed laws equating the use of a digital certificate with that of appearing before a Notary Public. The National Notary Association argues in *A Position on Digital Signature Laws and Notarization* that the role of the Notary Public is critical and that physical presence is critical and cannot be replaced by technology. According to the NNA, "the complexity of digital signature technology heightens rather than diminishes the role of the Notary.[1]" The Commonwealth Joint Commission on Technology and Science (JCOTS) has formed an advisory committee on electronic government, which will examine the role of Notary Publics. The Secretary of the Commonwealth has formed an advisory committee on this topic with representation from the DSI Workgroup.

- **Online voting.** Citizens are clamoring for voter registration and online voting applications, especially in congested areas and remote rural locations. While there has been discussion about electronic voting, there have been only a few attempts to implement it. And while some polls show that electronic voting is a top choice of respondents, suspicions remain that votes cast via the Internet may not be secure and confidential. An electronic voting system design must reflect the need for absolute security, secret ballots, prevention of multiple voting and voting fraud, and checks for voter eligibility. Further, it must ensure that information related to the individual voter is rendered anonymous and irretrievable, and that the vote is transmitted secretly and accurately. For more information on electronic voting, see *Appendix K: Electronic Voter Registration and Electronic Voting*.

…there are significant opportunities for linking, leveraging, and leadership on the horizon.

- **New business models.** Opportunities to provide certification authority and registration authority services to the general public are being explored internationally by banks and financial institutions. Nationally, the U.S. Postal Service (with Imagitas of Boston) envisions GovKey—a digital certificate program designed to boost e-government services between government (federal, state, and local) and citizens. In the GovKey model, the U.S. Postal Service would serve as the registration authority, with more than 38,000 local post offices nationwide.
- **Federal and International Initiatives.** The General Services Administration (GSA) has created the Access Certificates for Electronic Services (ACES) program to promulgate digital certificates among federal agencies. ACES participants include the Federal Emergency Management Agency, the U.S. Department of Education, the U.S. Department of Labor, the U.S. Department of Veteran Affairs, the U.S. Postal Service, the U.S. Environmental Protection Agency, the National Institutes of Health, and the Social Security Administration. GSA's Federal Electronic Commerce Program is identifying crosscutting applications—applications that transverse federal, state, and local lines. See *Appendix X: International Digital Signatures Efforts* for information on deployments in other countries.
- **DMV as registration authority.** The California legislature is considering action to designate the California Department of Motor Vehicles the state's Registration Authority. The primary role of an RA is to verify and authenticate identity—a process DMV uses in issuing state identification cards and driver licenses. Any DMV considering such a proposal should first examine a number of policy, operational and support areas: levels of assurance in its existing identification verification process, liability issues, program funding, fee structures, staffing needs, privacy concerns, IT system configurations, and data security and audit processes.

Evolving Standards and Technologies

- **Electronic forms and workflow software.** Electronic forms, or e-forms, are PKI-enabled software packages for implementing electronic forms. E-forms packages are generally not end-to-end business solutions in and of themselves—they are a component of this solution. The ability to obtain the greatest value from e-forms will depend on how the package is architecturally positioned. Recommended attributes include forms delivery by an intranet, interoperability, and XML support.
- **Biometrics.** Biometrics is technologies for measuring and analyzing biological characteristics—such as a fingerprint, the retina or iris, facial patterns, and voice or handwriting patterns—to authenticate identity. For maximum security, biometrics could be used in combination with digital signatures and other electronic signatures.
- **Smartcards and alternative hardware tokens.** A smartcard is usually the size of a credit card and contains a microchip where data—such as the private key and digital certificate—can be stored. Other hardware tokens, such as key fobs, offer similar security benefits. Like ATM cards, smartcards are less vulnerable to attack than browsers, and are portable.
- **Encryption.** Encryption is a method of protecting data by converting data into an unintelligible form that can only be returned to a readable state by using a special key or password to decrypt or decode it.

Encryption is used to protect data while it is in transit and also when it is resident within a system or in storage.

- **Document management.** Once a document is digitally signed and delivered, there are a host of considerations for filing, retrieving, and restoring documents to conform to the Virginia Records Retention and Disposition Schedules. Converting manual documents to electronic form, can be a challenge since a change in technology can render documents unrecoverable that are stored on older technology. A decision to move forward with manual to electronic conversion should be accompanied by a decision on how converted documents will be stored, kept technically current, and eventually deleted at the end of their life cycle.
- **Toward single sign on (SSO).** A number of tools and methodologies exist which could help enable SSO, including meta-directories, attribute certificates, and privilege management infrastructure. Digital signatures and PKI do not, in and of themselves, provide SSO capability, but they can be SSO-enabled to help move the environment toward SSO capability. For more information, see *Appendix Y: Attribute certificates* and *Appendix Z: Positioning the Commonwealth for Single Sign On*.

For more detailed information on emerging models and evolving standards, see *Appendix AA: Digital Signatures Horizons Issues*.

A number of tools and methodologies exist which could help enable single sign on....

[1] National Notary Association. "A Position on Digital Signature Laws and Notarization." July 20, 2000.

IX. TOOLS AND RESOURCES

As a result of the DSI effort, we have developed a number of tools and guidelines, and developed a substantial base of knowledge to advance the Commonwealth toward the Governor's vision for The Digital Dominion. In particular, we have:

Solutions

- A simplified, vendor-neutral trust architecture model based on open standards.
- A flexible business model to guide implementation of digital signatures that can meet the needs of the Commonwealth as an enterprise as well as the needs of its disparate organizational components.
- Principal role definitions for moving forward in a coordinated, strategic manner with multiple partners.
- An acquisition strategy with selected supporting reference materials to inform and guide deployment decisions.
- A plan of action synergistic with other COTS endeavors and initiatives at all levels in the public and private sectors.
- An enterprise solution to offer agencies, localities, and higher education that provides the best business case for adopting digital signature technology.

A simplified, vendor-neutral trust architecture model based on open standards.

Tools

- Step-by-step business decision criteria to guide decision-makers in determining whether digital signature technology is appropriate.
- A cost model that highlights direct and opportunity costs, and the major cost considerations in deploying digital signature technology.
- Audit and assurance best practices and standards to ensure proper controls are put into place to protect transactions, prevent fraud, and provide an audit trail.
- Key technical standards to promote interoperability and provide high levels of assurance.

Resources

- Experience-based knowledge and skills developed through the robust demonstration effort and by building on the knowledge and experiences of others nationally and internationally.
- An informed perspective on evolving issues and trends.
- Contacts in multiple states, the federal government, and the Government of Canada.
- Strong industry relationships with digital signature and PKI vendors and experts.

X. Plan of Action

The DSI Workgroup recommends the following action steps.
(See *Appendix BB: Time-Phased Action Plan*.)

I. The Secretary of Technology should reestablish the Digital Signatures Workgroup to consist of the VOLT Governance Group, the DS Procurements Team and other sub-units to support the proposed deployment effort. The new DS Deployment Workgroup should oversee the RFP development process and coordinate the resolution of legal, policy, and technical issues

Timeframe: October 2000

II. DIT should procure a vendor source or sources for an array of enterprise products and services related to PKI and digital signatures, including CA services (prominently featuring VOLT-standard products) and all based on DSI findings and recommendations. DIT should work with the DS Deployment Team to develop a concept of operations and articulate the VOLT open standards. Applications and platform integration services should be procured in the same manner.

RFP Development: October 2000 – January 2001
Issue RFP(s): January 2001
Award RFP(s): June/July 2001

III. The standards and best practices recommended by the DSI Workgroup should be adopted through the Secretary of Technology, most notably those applying to the VOLT Certificate, its assurance levels, audits and controls, storage of private keys, and recommended limits on the use of document encryption for storage.

October 2000

IV. A source of funding should be sought by the Secretary of Technology.

October 2000

V. Appropriate staffing should be supplied for the effort through the Secretary of Technology, most notably legal counsel and project management.

October –November 2000

VI. The proposed digital signature deployment timeline should be adopted by and promoted as a priority to Secretary of Technology agencies.

October 2000 – January 2001

VII. Early Adopter candidates—Executive Order 65 administrative applications, agencies, localities, and the educational community—should be recruited selectively by the Digital Signature Deployment Workgroup and commissioned by the Secretary of Technology.

October 2000 – January 2001

VIII. The COTS Executive Committee should proactively exploit synergies the Digital Signature Initiative has identified with other COTS initiatives and align priorities and resources to boost momentum toward the Administration's vision for the Digital Dominion.

October 2000 and ongoing

IX. The Department of Technology Planning and the Electronic Government Implementation Division should develop a training program and a promotional and security awareness campaign that takes advantage of the DSI findings and lessons learned.

October 2000 – January 2001

X. The DS Deployment Workgroup should actively monitor ‘horizon’ issues and work through COTS to adjust for and to leverage these developments.

October 2000 and ongoing

Conclusion. As a result of the DSI Workgroup’s inquiry, the Commonwealth is positioned to assume a leadership role in deploying digital signature technology strategically to improve services to citizens, realize cost-savings benefits, and reap the benefits of electronic government.

As a result of the DSI Workgroup’s inquiry, the Commonwealth is positioned to assume a leadership role in deploying digital signature technology strategically to improve services to citizens, realize cost-savings benefits, and reap the benefits of electronic government.

XI. Appendices

The Appendices contain source documents authored during the course of the Digital Signatures Initiative inquiry. ***The documents do not necessarily reflect the opinions or views of the Digital Signatures Initiative Workgroup or the current thinking or direction of Workgroup activities.*** The source documents are provided strictly as a means of documenting the efforts of the Workgroup as it formed its findings, conclusions, and recommendations, and, in some instances, serve as resources for the proposed development effort.

Unless otherwise noted, the appendices were developed by the DSI Workgroup staff. The thirty appendices include the following documents:

- *Digital Signatures Initiative Deliverables* illustrates the specific charge of the DSI Workgroup in relation to Executive Orders 51 and 65.
- The *Glossary of Terms* provides definitions of digital signature-related terms and phrases.
- The *Frequently Asked Questions* appendix contains general questions (and their answers) about digital signatures and the DSI effort in the Commonwealth of Virginia.
- The *DSI Calendar of Events* chronicles the major activities and meetings of the DSI Workgroup.
- *Works Cited and Further Reading* lists books, publications, articles, links to web sites (organized by category) for more information on a given subject.
- The *State Audit Survey* Summary describes the results of a survey conducted on behalf of the Audit & Assurance Team to measure audit involvement in digital signature efforts in more than twenty other states and monitor overall deployment progress.
- The *DSI Demonstration Projects* contains an overview of each pilot project, lessons learned, and more detailed information about each pilot project.
- The *Commonwealth Bridge Certification Authority* appendix describes the bridge prototype developed by the University of Virginia based on the Federal Bridge Certification Authority project.
- The *Digital Signatures Business Case* highlights the benefits and advantages of employing digital signatures by agencies, institutions, and localities.
- The *Digital Signatures Decision Model* provides criteria to help decision-makers determine whether a specific transaction is a suitable candidate for digital signatures.
- *Comparison of Electronic Signature Legislation* provides a point by point comparison of the Federal E-Sign Act, the national UETA model, and the Virginia UETA.
- *Electronic Voter Registration and Electronic Voting* appendix provides detailed information on the obstacles and opportunities for deploying electronic voting technologies and policies. E-voting provides an excellent example of the numerous systemic obstacles to e-government—policy decisions and barriers, cultural resistance, and technical challenges.
- *Executive Order 51 Review* includes a summary of the plans agencies and institutions filed per Executive Order 51 detailing their plans for employing electronic and digital signatures.
- *VOLT Open Standards Proposal* describes an approach to setting standards in the Commonwealth to achieve the highest levels of assurance while promoting interoperability and providing simplicity and flexibility.
- *Internal Control and Auditing Standards* was developed by the Audit & Assurance Team to provide an audit control framework for digital signatures in the Commonwealth.
- *Legislative Environment* describes recent legislation passed nationally and in the Commonwealth of Virginia. Developed by the Audit & Assurance Team, the appendix offers a number of findings and recommendations for overcoming legal and regulatory obstacles.
- *RFP Resources* provide a number of source documents to help inform the procurement process for certification authority services and PKI products.

- *Proposed Digital Signatures Deployment Workgroup Organization* chart displays the proposed reconfiguration of the DSI Workgroup into several teams.
- *VOLT Early Adopters Program Concept Paper* highlights the major components of the Early Adopters Program, based on the models in Washington and Illinois states.
- *Concept of Operations Outline* is a working template for articulating the vision of and standards for an enterprise-wide digital signatures solution.
- *Proposed VOLT Governance Charter* describes the role and responsibilities of the VOLT Governance Team, which will provide oversight and governance to the digital signatures efforts in the Commonwealth.
- The *Digital Signatures Cost Model* identifies the major cost components for implementing digital signatures solutions.
- The *Health Insurance Portability and Accountability Act* appendix describes the basic tenets of HIPAA and how the forthcoming regulations could affect Commonwealth agencies.
- *International Digital Signatures Efforts* describes the initiatives underway throughout the world.
- *Attribute certificates* is a concept paper describing the benefits of attribute certificates.
- *Positioning the Commonwealth for Single Sign On* provides recommendations for steps the Commonwealth should take to use PKI and digital signatures to move toward single sign on capability.
- *Digital Signatures Horizons Issues* describes some of the major emerging practices, models, and technologies.
- The *Time-Phased Action Plan* illustrates the major action steps for the deployment effort.

DIGITAL SIGNATURES INITIATIVE DELIVERABLES

AUGUST 15, 2000

COTS/PSA DIGITAL SIGNATURE REPORT • 10/99		**EXECUTIVE ORDER 51 • 7/23/99**		**EXECUTIVE ORDER 65 • 5/24/00**
DELIVERABLES (6)	COMP.	DELIVERABLE S	COM P.	DELIVERABLE S (9)
— N/A —		The Secretary of Technology shall submit a report to the Governor by 11/1/99 concerning plan to facilitate the use and authentication of electronic signatures. (I.)	✔	— N/A —
Establish the Digital Signature Initiative Workgroup to demonstrate use of digital signatures internally within an agency, agency to agency, agency to business partners, and agency to local government, and to report on results. (6)	✔	— N/A —		The Secretary of Technology/eGov will coordinate with the Council on Technology Services regarding the development of the related policies, standards, and guidelines necessary for statewide deployment of digital signatures. (6)
-N/A-		-N/A-		The Secretary of Technology/eGov will receive advice and assistance from COTS in regard to the Commonwealth's implementation of the initial demonstration projects. (5)
A demonstrated working *solution of trust* and confidence extensible to the Commonwealth public sector community, to business partners and to the public. (5)		— N/A —		Development of a demonstrated working model that allows for the verification of digital signatures that can then be extended to the Commonwealth's public sector community, to business partners, and to the general public. (4)
A Commonwealth Bridge Certification Architecture. (3)		— N/A —		Development of a digital signature structure that can support the use of more than one Certificate Authority. (3)
An enterprise technical architecture and acquisition strategy based on experience. (2)		— N/A —		Application of a proven operating environment that supports the use of secure digital signature technology and could later be applied statewide. (2)
A foundation of policies, practices, guidelines and standards necessary to transition into an enterprise production environment. (1)		— N/A —		Establishment of policies, practices and guidelines that will serve as the basis for applying digital signatures statewide. (1)

COTS/PSA DIGITAL SIGNATURE REPORT • 10/99		EXECUTIVE ORDER 51 • 7/23/99		EXECUTIVE ORDER 65 • 5/24/00
DELIVERABLES (6)	COMP.	DELIVERABLE S	COM P.	DELIVERABLE S (9)
An invested knowledge and skills base for decision makers and technical staff. (4)		-N/A-		-N/A-
-N/A-		-N/A-		The Secretary of Technology/eGov will encourage appropriate Executive Branch agencies and institutions to take advantage of digital signature technology. (8a)
		— N/A —		The Secretary of Technology/eGov will develop an educational program for agencies, institutions of higher education, and local governments on how to implement secure digital signature technology. (8b)
— N/A —		— N/A —		The Secretary of Technology/eGov will coordinate with the appropriate Executive Branch agencies to facilitate the procurement activities relating to statewide deployment of digital signature technology. (7)
— N/A —		— N/A —		The Secretary of Technology/eGov will ensure that implementation of digital signature technology by the Commonwealth complies with the provisions of the Uniform Electronic Transactions Act of 2000. (9)
-N/A-		-N/A-		The Governor directs Executive Branch agencies and institutions to take advantage of the benefits of digital signature technology to the fullest extent possible.
— N/A —		Agencies must incorporate guidance from the Sec. of Technology on use of electronic signature technology into their proposed plans for Web-enabled internal/external transactions. (J.)		— N/A —

APPENDIX B

GLOSSARY OF TERMS

October 16, 2000

Algorithm: A finite series of steps or processes that terminates with an answer. Digital signatures rely on mathematical algorithms.

Asymmetric cryptography: In asymmetric cryptography, the key used to scramble (encrypt) data is not the same key used to unscramble (decrypt) the data. Digital signatures rely on public key cryptography—a form of asymmetric cryptography—where mathematically-related key pairs are generated. Information that is encrypted with one of the keys can only be decrypted by using the other key.

Authentication: The process of determining whether or not someone (or something) is what or what it claims to be. In private and public computer networks, authentication is commonly done through use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. The weakness in this system is that passwords can often be stolen, accidentally or purposefully revealed, or forgotten.

For this reason, Internet business and many other transactions require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a Public Key Infrastructure (PKI) is considered to be the future of authentication on the Internet. Logically, authentication precedes authorization (although they may often seem to be combined).

Authorization: The process of giving someone permission to do or to have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use they have (such as access to which file directories, hours of use, allocated storage space, etc.).

Certificate or Certification Authority (CA): The authority in a network that issues and manages security credentials and public keys for message encryption and decryption. It issues secure electronic identities to users in the form of certificates. In creating certificates, CA's act as agents of trust in a Public Key Infrastructure (PKI) by signing the digital certificates. As long as users trust a CA and its business policies and practices for issuing and managing certificates, they can trust the certificates issued by that CA.

Certificate or Certification Policy (CP): The statement that governs all aspects of CA functions, including the general characteristics and structure of digital certificates, identification and authentication methodologies, and certificate life cycle management.

Certification Practice Statement (CPS): A comprehensive description of how all policy requirements stated in the certificate policy will be implemented and maintained by a CA.

Ciphertext: Plain text that has been encrypted, or made unreadable, through use of an algorithm.

Confidentiality: The assurance that information received or sent is not disclosed to inappropriate or unauthorized entities or processes.

Certificate Revocation: To permanently cancel a certificate. The revoked certificate, along with the necessary information identifying the certificate holder, will be placed on the certificate revocation list (CRL) maintained by the certificate authority (CA). Messages sent and transactions conducted under a revoked certificate will not be honored, and will be denied (not accepted) by the recipient.

Certificate Revocation List: A list of all cancelled certificates, maintained by the certificate authority. This list is automatically accessed as a part of the verification process.

Cross-Certification: A process in which two CA's securely exchange keying information so that each can effectively certify the trustworthiness of the other's key. Essentially, cross-certification is an extended form of third-party trust in which network users in one domain implicitly trust users in all other CA domains that are cross-certified with their own CA.

Data Integrity: A measure of the reliability of data based on a series of security measures taken to prevent data-tampering and unauthorized alterations. Assuring data integrity is critical to supporting non-repudiation and confidentiality.

Decryption: The process of converting encrypted data back into its original form so that it can be understood. Presumably, only the generator of the file and the authorized recipients can decrypt the file. Decryption is accomplished by using a key or algorithm that undoes the work of the encryption key and algorithm.

Digital Certificate: An electronic credential for conducting business or other transactions on the Web. Digital certificates are issued by a certification authority (CA). Digital certificates contain identity information, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the issuing CA. The digital certificate allows the recipient to verify that a digital signature is valid and trustworthy. Digital certificates provide a registered identity to users to ensure that other parties with whom they communicate are "safe." These identities are proven trustworthy since the CA (the trust agent in the PKI) signs the digital certificates before issuing them.

Digital Signature: An electronic, rather than a written, signature. A digital signature (not to be confused with a digitized signature) is one form of electronic signature. Digital signatures are used to authenticate the sender of a message or the signer of a document, ensure that the original content of a message or document is unchanged, and support non-repudiation.

Digitized Signature: An electronically recorded handwritten signature. Unlike digital signatures, digitized signatures do not ensure data integrity or non-repudiation.

Directory Services: These services are necessary for the full functioning of a public key infrastructure (PKI). The directory holds the user's certificates, which contain their public keys. Also, the directory contains the list of revoked certificates (CRL lists). The Directory is an important piece of the PKI infrastructure, as the public keys it contains are accessed frequently for the following purposes:

- **Verifying digital signatures.** Public keys are necessary to verify digital signatures (i.e., authenticate the identity of the sender and verify the integrity of the document).
- **Checking for revoked certificates.** Interaction with users whose certificates have been revoked should not occur.
- **Decrypting messages.** Public keys stored in the certificates on the directory are accessed to allow a sender to be able to encrypt a message using the public key of the recipient, thereby ensuring that the message can only be decrypted with the recipient's private key.

Electronic Signatures: Any symbol applied electronically to a record indicating intent to sign. Digital signatures is one form of electronic signature—other forms include personal identification numbers (PINs), passwords, pass phrases, biometrics, and other hardware tokens such as smartcards.

Encryption: The conversion of data into a form called ciphertext that cannot be easily understood by unauthorized persons. To encrypt a file is to apply a mathematical function that transforms every character in the file into some other character. Encryption renders the file unreadable. This means no one, including the recipient, can read the file until it is decrypted, or conformed back into the original characters. As long as the decryption key is held securely only by those who should have it, only the authorized recipients can decrypt the file.

Firewall: A set of related programs, located at a network gateway server, that protects the resources of a private network from users of other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources, and for controlling what outside resources its own users have access to. The firewall screens and filters incoming requests before routing them to internal locations.

Gateway: The network point that serves as the entrance to another network. On the Internet, the network consists of gateway nodes and host nodes. The computers of network users and the computers that serve content (such as Web pages) are host nodes. The computers that control the traffic with your company's network or at your local Internet service provider (ISP) are gateway nodes. In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server as well.

Hash Function: An algorithm used to encode a string of characters (such as a message or document) into a shorter, fixed length, encoded message. The hash function performs a mathematical summary of the document resulting in what is known as a hash code or message digest. This hash code is a unique identifying digital fingerprint of the document or message and has the following characteristics: 1) if the message or document changes even by one character, the hash code will dramatically change, 2) the original message can not be recreated from the hash code, and 3) the probability that any two arbitrary documents will produce the same message digest is very, very small.

Interoperability: The ability of a system or product to work with other systems or products without special effort by the user. Interoperability is achieved by relying on industry standards or by using a central "broker" that converts data into a usable form. In the digital signature environment, interoperability also refers to commonly understood means to verify certificates (trust paths) and to policy mapping. Two CAs, for example, may use the same products but have different certificate policies. Though the certificates are interoperable from a technical point of view, they may not be accepted in the other CA environment due to a lack of ability to "map" the two certification policies to each other (proving they are "equivalent" to each other in all respects that are judged important by the relying party).

Key: A large number that is used by an algorithm to encrypt text. The length (size) of the key generally determines how difficult it will be to decrypt the text of the message.

Key Pairs: Key pairs are mathematically related key sets consisting of a private key and a public key. Though the key pairs are inextricably linked, the private key cannot practically be derived from the public key alone.

Online Certificate Status Protocol: The Online Certificate Status Protocol (OCSP) enables applications to determine the state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response. This protocol specifies the data that needs to be exchanged between an application checking the status of a certificate and the server providing that status.

Non-Repudiation: Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.

Privacy: The ability of an individual or organization to control the collections, storage, sharing, and dissemination of personal and organizational information.

Private Keys: The private key in a public/private key pair is generated by the CA or by the user's system. The private key is used to apply digital signatures and to decrypt data that was encrypted with the corresponding public key. Because digital signatures are legally binding and indicate intent to enter into a contract or agreement with another party, it is critical to non-repudiation that the private key is stored securely and kept under the sole control of its owner.

Proxy server: A server that acts as an intermediary between a workstation user and the Internet, so that the enterprise can ensure security, administrative control, and other services.

Public Key Cryptography: The primary feature of public key cryptography is that it removes the need to use the same key for encryption and decryption of information. With public key cryptography, keys come in matched pairs of public and private keys. See **asymmetric cryptography** for more information.

Public Keys: The public key in a public/private key pair is generated by the CA or by the user's system. The public key is used to verify digital signatures and to decrypt data that was encrypted with the corresponding private key. Public keys are contained in certificates that are issued by a Certificate Authority (CA) after verifying the identity of the owner of the public key. The receipt of a digitally-signed document uses the sender's public key to verify the validity of the signature and ensure the data has not been tampered with.

Public Key Infrastructure (PKI): A comprehensive system required to provide public key encryption and digital signature services. It enables users of a basically unsecured public network such as the Internet to exchange data and money securely and privately through the use of a public and private cryptographic key pair that is obtained and shared through a trusted authority. The purpose of a public key infrastructure is to manage keys and certificates. By managing keys and certificates through a PKI, an organization establishes and maintains a trustworthy networking environment. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

A public key infrastructure consists of:

- A certificate authority (CA) that issues and verifies digital certificates. A certificate includes the public key and identifying information about its owner. The private key is under the sole control of the requestor.
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor.
- PKI-enabled applications.

Registration Authority: The registration authority (RA) refers to the people, processes, and tools used to support the registration of users with the PKI (enrollment) and ongoing administration of users. The RA is the authority in a network that verifies user requests for a digital certificate and then tells the certificate authority (CA) to issue it. RAs are part of a public key infrastructure (PKI).

Relying party: A Relying Party is a person, entity, or organization that relies on or uses a digital certificate any other information provided in a repository or database to verify the identity and public key of another user.

Root key: The root key is the CA’s private signing key, which is used to issue digital certificates.

Standards: An agreed upon set of rules, guidelines, procedures, policies, and practices to promote interoperability.

Symmetric Cryptography: The same key is used to scramble (encrypt) and unscramble (decrypt) data. The weakness of symmetric cryptography is the difficulty of transferring the symmetric key from sender to recipient securely so that the recipient can use that key to decrypt data.

Time Stamp: A notation added to a document, especially an encrypted one, that indicates, at a minimum, the date and time of an action, and the identity of the person that created the notation. A time stamp is most frequently used for documents such as contracts or proposals where the exact time filed or submitted is of critical importance.

APPENDIX C

FREQUENTLY ASKED QUESTIONS

September 25, 2000

What initiatives have been undertaken in Virginia to explore the use of digital signatures?

In November of 1998, several Council on Technology Services (COTS) work groups were designated to explore and address a variety of technology issues which most affect the quality, convenience, and efficiency of service delivery by Virginia government. Among these was the Privacy, Security and Access (PSA) work group. In late May 1999 the issue of digital signatures for the Commonwealth was identified as a priority for the PSA work group. Between June and October the work group researched and dialogued with local, state, federal and industry colleagues about digital signatures and Public Key Infrastructures. As a result of findings from the PSA work group it was recommended that a separate work group be formed to proceed with enabling PKI/digital signatures.

This Digital Signature Initiative (DSI) work group was formed and began meeting in December 1999. The work group included members from five agencies, four localities, one university, and VIPNet (Virginia Interactive, L.L.C.). Working in collaboration with the work group members were industry representatives, an Audit & Assurance Team consisting of agency, university and locality representation, and various PKI and digital signature experts. Eleven demonstration projects ran from June to August 2000. Experiential lessons learned from these demonstrations and research conducted provided the necessary information for recommendations and findings of the DSI Work Group as presented in *Digital Signatures Initiative: An Enterprise Solution of Trust.*

What is the legal status of digital signatures in Virginia?

The use of digital signatures in the State of Virginia is addressed in the Uniform Electronic Transactions Act (HB499) under the definition of electronic signatures. This legislation adopts the Uniform Electronic Transactions Act (UETA) promulgated by the National Conference of Commissioners on Uniform State Laws. The highlights under Virginia's UETA are: a record or signature may not be denied legal effect or enforceability solely because it is in electronic form; a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation; if a law requires a record to be in writing, an electronic record satisfies the law; and, if a law requires a signature, or provides for certain consequences in the absence of a signature, an electronic signature satisfies the law.

What is the legal status of digital signatures in the Federal Government?

The Electronic Signatures in Global and National Commerce Act, S.761, commonly known as the "e-Sign bill" was signed into law on October 1, 2000. This legislation makes electronically signed transactions legally binding the same way paper documents with handwritten signatures are binding today. It covers not only services given by government to consumers and businesses, but also business-to-business and business-to-consumer transactions. It paves the way for a uniform legal framework of consistent rules for using and validating electronic signatures to conduct e-business. And, it will allow companies to begin replacing paper records with electronic ones.

What is a digital signature?

A digital signature is a convenient, secure, and reliable method of signing electronic documents that provides the recipient with a way to verify the sender, determine that the content of the document has not been altered since it was signed and prevent the sender from repudiating the fact that he or she signed and sent the electronic document. A digital signature is the encrypted version of the message digest of the signed document. The encryption is performed using the signer's private key. The signature is verified using the signer's public key.

What is an electronic document?

An electronic document is any document generated or stored on a computer. An electronic document may be an email message, a contract, a purchase order, a letter or some other type of document. An electronic document can also be an image such as a drawing or photograph. A digital signature can be used to sign or authenticate all of these types of electronic documents.

What is a public key? What does it do?

The public key is the part of the key pair used by the recipient of an electronic document to verify the sender's signature. It is maintained in a digital certificate issued by the certification authority. The public key is available for use by anyone wishing to authenticate documents you sign.

What is a private key? What does it do?

A private key is the part of the key pair that is used by the person to sign an electronic document. It must be kept secure and under the sole control of its owner as it is considered the identity of the person in the electronic environment. The private key is used only by its owner and is required during the signing process. It can be stored either in your computer or on various hardware devices.

What is PKI (Public Key Infrastructure)?

A Public Key Infrastructure (PKI) enables effective integration of digital signatures and encryption for business processes to deliver user-friendly, efficient, and reliable data and network security enterprise-wide. A comprehensive PKI includes the technology, infrastructure, and practices that are needed to issue, manage, and process various types of digital certificates. A PKI also involves maintaining user records and directories, as well as distributing and managing private and public keys.

What are the key components to a PKI?

A PKI requires a Certification Authority (CA) and a Registration Authority (RA). The CA is the trusted third-party that issues certificates to users and handles multiple administrative tasks, including key management, certificate validation, key expiration and revocation, key updates, key recovery, policy administration, and maintenance. The RA must first vouch for the identity of an individual before a certificate is issued.

If my private key is stored on my computer, can't someone sign documents without my permission by getting access to the computer?

No. Your private key is encrypted when it is stored on your computer. When you sign an electronic document, you enter an authorization code (password) to decrypt the private key for as long as it takes to sign the document.

If someone learns of your authorization code and also has access to the computer holding your private key, the integrity of your private key is compromised. In this case you would want to have your digital signature certificate revoked and obtain another. This would be the same as reporting a stolen or lost credit card.

What is a digital certificate and why is it so important?

Just as a driver license or passport identifies a person in a face-to-face transaction, a digital certificate identifies a person and gives security assurance in transactions over the Internet. A digital certificate ensures authenticity, privacy and accountability in electronic transactions, and can be used to verify a legally binding digital signature.

A digital certificate is a unique digital ID for an individual, group or organization. The digital certificate contains information about the holder (such as the person's name and a copy of their public key), various attributes (such as expiration date and serial number), and the certification authority guaranteeing the authenticity for this certificate. Digital certificates can be stored in browsers, on disks, or in directories. Digital certificates allow senders and receivers of digital information to be confident of the identity of the party they are dealing with.

How do I get a digital certificate?

When you choose your digital signature software, it may come with an application for the certificate. The application requests information used to verify your identity and protect you against unauthorized use of your signature. You may also obtain a certificate directly from a certification authority.

What is the responsibility of a digital certificate holder?

The certificate holder is responsible for safeguarding access to their private key.

What does a digital signature look like?

A signature looks like a random series of numbers and alphabetical characters. Each signature is unique because it is the encrypted version of the message digest of the electronic document being signed.

An example of a digital signature is:

```
------BEGIN SIGNATURE -----------
idkflkmejsdaoif344lklkrlk08+kadlkdflioe993+lalkfdlasd
4ksrlk4lksafj8lkadfkl6lafdlfj+kdakljfl6ladfldfjl+adfsdfddf+
------ END SIGNATURE ---------------
```

How does a digital signature work?

A digital signature is more of a process than just affixing a signature. For example, when the document is digitally signed, the digital software scans the document and creates a message digest (hash code) which represents the document. This message digest is then encrypted with the signer's private key. When the recipient authenticates the signature, a similar process is carried out. The sender's and the receiver's message digests are then compared. If the results are the same, the signature is valid; if they are different, the signature is not valid.

If a digital signature is used, can you actually see the signer's handwritten signature?

No. There is no relationship between a handwritten signature and a digital signature. What you can see if a digital signature is used is the signer's name, the certificate serial number and the certification authority's name. You may also be able to see additional information, such as title and organization name, depending on the certificate content protocols or standards used. This is determined in accordance with the subscriber's certificate policy.

Can a digital signature be forged?

Not likely. It is protected by several layers of highly complex encryption. With digital signatures, forgery is next to impossible.

Can my digital signature be stolen?

Your digital signature can only be stolen if you lose control of or divulge your private key. If this happens, it must immediately be reported to the certification authority.

Why are digital signatures so important?

Digital signatures are likely to dramatically alter the way the world communicates. Essentially, this technology will allow us to conduct legally-binding, paperless communications and commerce on a worldwide basis.

Why should we use digital signatures?

Many organizations are now interested in technologies that can help them reduce their dependency on paper and its associated costs. This is true of governments and the business world. Digital signatures can potentially be used in many different ways, including: granting access to electronic resources without requiring user ids, adding security to email, and signing electronic forms. The move away from paper is expected to reduce storage costs, to decrease the time it takes to move forms through the work flow, and to eliminate mailing costs.

How do I know that the digital signature received from a sender is valid?

Part of a certification authority's responsibility is to revoke, expire, or suspend certificates upon direction of the certificate holder or the organization to which they belong. These revocations, expirations, and suspensions are submitted by the CA either on a regular basis to a Certificate Revocation List (CRL) or can be updated automatically via the Online Certificate Status Protocol (OCSP), which provides real-time validation of a certificate's status.

DSI CALENDAR OF EVENTS

October 17, 2000

1999

DECEMBER

December 7 – DSI Workgroup meeting held at DMV, Room 702 from 9 a.m. to noon.

2000

JANUARY

January 21 – DSI Workgroup meeting held at DMV, Room 702 from 9 a.m. to noon.

FEBRUARY

February 20 – DSI Workgroup meeting held at DMV, Room 702 from 9 a.m. to noon.

MARCH

March 9 – DSI Workgroup meeting held at DMV, Room 702 from 9 a.m. to noon.

March 15 – Education Day held at the University of Virginia in Charlottesville from 9 a.m. to 4:00 p.m. Primary focus was on issues and questions specifically relating to the State of Virginia pilot agencies participating in the digital signature initiative sponsored by the Council on Technology Services.

APRIL

April 18 – DSI Workgroup meeting held at DMV, Room 702 from 9 a.m. to noon.

April 26 – RSA Security hosted a free half-day **PKI Seminar** in Washington D.C.

MAY

May 11 – Meeting at the Department of Game & Inland Fisheries. This meeting was held for all pilot project participants and Entrust Technologies. The purpose of the meeting was to resolve technical questions about the pilot projects.

May 15 – Meeting at the Department of Information Technology. This meeting was held for all pilot project participants. The purpose was to explain DIT's pilot project with expected project dates along with discussion of it's design and process flow.

May 18 – Meeting at the Department of Game & Inland Fisheries: Bridge meeting—principal participants were UVA, VIPNet, DGIF, and an Entrust systems engineer. The purpose of the meeting was to resolve all remaining technical issues about the bridge.

May 25 – KPMG hosted a full-day training session for the Audit & Assurance Team on PKI/Audit & Standards Issues in Richmond, Virginia.

May 26 – DSI Workgroup meeting held at DMV, Room 702 from 8:30 a.m. to noon.

JUNE

June 20 – DSI Workgroup meeting held at DMV, Room 702 from 8:30 a.m. to noon.

June 22 – Audit & Assurance Team meeting held at DMV, Room 730E from 1-5 p.m.

June 29 – Audit & Assurance Team meeting held at DMV, Room 702 from 1-5 p.m.

JULY

July 6 – Audit & Assurance Team meeting held at DMV, Room 730E from 1-5 p.m.

July 13 – DSI Workgroup/Audit & Assurance Team meeting and Parikh demonstration at Parikh Laboratories in Glen Allen, Virginia.

July 18 – DSI Workgroup meeting held at DMV, Room 702 from 8:30 a.m. to noon.

July 20 – Audit & Assurance Team meeting held at DMV, Room 730E from 1-5 p.m.

July 27 – Audit & Assurance Team meeting held at DMV, Room 702 from 1-5 p.m.

July 27 – State Board of Election & Registrars Conference in Williamsburg, Virginia. The focus of this conference was on electronic registrations and on-line voting. Chip German represented the DSI Workgroup.

AUGUST

August 3 – Audit & Assurance Team meeting held at DMV, Room 702 from 1-5 p.m.

August 8 – Audit & Assurance Team meeting held at DMV, Room 702 from 1-5 p.m.

August 10 – DSI Workgroup meeting held at DMV, Room 702 from 8:30 a.m. to noon.

August 17 – Audit & Assurance Team meeting held at DMV, Room 730E from 1-5 p.m.

August 18 – DSI full-day work session held at DMV, Room 635 from 9-4 p.m., to consolidate issues and reach a first level of consensus on the COTS/DSI Report. Representative team (state agency, locality, education & CA's): Ray Lindquist (VDOT), Jim MaGill (Fairfax Co.), Chip German (UVA), Jim Adams (DIT), Cheryl Clark (DMV), Jennifer Wootton (DMV) and Diane Horvath (VIPNet).

August 24 – DSI/COTS Report Team full-day work session held at DMV, Room 505 from 9-5 p.m. Purpose of meeting was to consolidate issues, identified gaps regarding the final draft for the COTS/DSI report. Members: Cheryl Clark (DMV), Diane Horvath (VIPNet), Chip German (UVA), Ray Lindquist (VDOT), Barbara Deily (UVA), Jim Adams (DIT), Jim MaGill (Fairfax Co.), Jennifer Wootton (DMV), Mark Dennis (ORC), Karen West (DST), Tom Grecu (DST), and Yurity Dzambasow (DST).

August 31 – DSI Full Workgroup met a DMV, Room 702 from 1-5 p.m. This was a half-day work session addressing closure to key findings and recommendations from the final COTS/DSI report.

SEPTEMBER

September 13 – Preview meeting for Secretary Upson on the COTS Digital Signature Workgroup's findings and recommendations. The meeting consisted of a demonstration of one of the workgroup's pilots.

September 14 – DSI Workgroup meeting held at DMV, Room 702 from 8:30 a.m. to noon.

September 27 – DSI Workgroup Executive Briefing to COTS at the COVITS Conference, Lexington, Va.

OCTOBER

October 17 – DSI Workgroup meeting held at DMV, Room 702 from 8:30 a.m. to noon. Final meeting of the DSI Workgroup and launch of the Digital Signatures Deployment Workgroup.

APPENDIX E

WORKS CITED AND FURTHER READING

October 25, 2000

WORKS CITED

Adams, C. and Lloyd, S. *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations.* Indianapolis, IN: McMillan Technical Publishing, 1999.

American Bar Association, Information Security Committee, Section of Science & Technology. "Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce." August 1, 1996.

Grant, G. L. *Understanding Digital Signatures: Establishing Trust Over the Internet and Other Networks*. New York: CommerceNet Press, McGraw Hill, 1998.

The Internet Society. "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC2527). 1999.

National Council for Science and The Environment. "RL30435: Internet and E-Commerce Statistics: What They Mean and Where to Find Them on The Web." Congressional Research Service Issue Brief. February 17, 2000.

National Notary Association. "A Position on Digital Signature Laws and Notarization." July 20, 2000.

Office of the Governor, Commonwealth of Virginia. "Executive Order 51 (99): Implementing Certain Recommendations by the Governor's Commission on Information Technology." July 23, 1999.

Office of the Governor, Commonwealth of Virginia. "Executive Order 65 (00): Implementing Electronic Government in the Commonwealth of Virginia." May 24, 2000.

Piper, F., Blake-Wilson, S., and Mitchell, J. *Digital Signatures Security & Controls.* Rolling Meadows, IL: Information Systems Audit and Control Foundation, 1999.

Privacy, Security & Access Workgroup, Council on Technology Services. "Toward the Use of Digital Signatures in the Commonwealth of Virginia." October 1999.

Robinson, B. "States Seeking Bridges so PKI Can Span Systems." *civic.com*, FCW Government Technology Group

U.S. Congress. "Electronic Signatures in Global and National Commerce Act." Senate Bill 761. January 24, 2000.

U.S. Department of Commerce. "The Emerging Digital Economy II: Electronic Commerce in the Digital Economy." June 1999.

U.S. Department of Commerce, National Telecommunications and Information Administration. "Falling Through the Net: Defining the Digital Divide." July 1999.

Xcert International, Inc. "Building Trust on the Internet: A Practical Guide to Public Key Infrastructure." 1999.

FURTHER READING

BOOKS & PUBLICATIONS

Ford, W. and Baum, M. S. *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption.* Prentice Hall, 1997.

Civic.com
www.civic.com

Earthweb
www.earthweb.com

Federal Computer Week
www.fcw.com

SC Magazine
www.scmagazine.com

TechRepublic
www.techrepublic.com

ZDNet
www.zdnet.com

GENERAL INTEREST ARTICLES

Armstrong, Illena. "PKI: Has it Truly Arrived Yet?" *Security Magazine.* August 2000.
www.scmagazine.com/scmagazine/2000_08/cover/cover.html

Berinato, Scott. "PKI Still Mired in Pilot Mode." *eWeek.* August 7, 2000.
http://www.zdnet.com/eweek/stories/general/0,11011,2612063,00.html

Berinato, S. and Fisher, D. "Cheaper Techniques Take on PKI." *eWeek.* August 21, 2000.
http://www.zdnet.com/eweek/stories/general/0,11011,2617314,00.html

Breed, C. and Murray, W. "PKI: The Myth, the Magic and the Reality." Earthweb.com. September 7, 1999.
http://www.earthweb.com/dlink.resource-jhtml.72.1293.|repository||common|content|article|19990907|cn_pkimyth|pkimyth~xml.0.jhtml?pageNo=1&cda=true

Harreld, Heather. "Security Complex." *civic.com.* August 7, 2000.
http://www.fcw.com/civic/articles/2000/august/civ-feature3-08-00.asp

Lemos, Robert. "Digital Signatures a Threat to Privacy?" *ZDNet News*. April 7, 2000.
www.zdnet.com/zdnn/stories/news/0,4586,2523596,00.html

Robinson, Brian. "States Seeking Bridges so PKI Can Span Systems." *civic.com.* August 7, 2000.
http://www.civic.com/civic/articles/2000/august/civ-tech-08-00.asp

Saunders, John. "Digital Signatures Promise Real Benefits for Washington." *Harddrive*. Summer 2000.
www.aamva.org/Publications/Harddrive/digital_signature_S00.html

INTERNET STATISTICS

eMarketer
www.emarketer.com/estats

Federal Bureau of Investigation and National White Collar Crime Center Internet Fraud Complaint Center
www.ifccfbi.gov/

GLG Consulting's Facts, Figures and Forecasts
www.glgc.com/fff.html

Headcount (Internet usage around the world)
www.headcount.com/

The Internet Economy Indicators
www.internetindicators.com/facts.html

The National Council for Science and the Environment. "RL30435: Internet and E-Commerce Statistics: What They Mean and Where to Find Them on the Web."
www.cnie.org/nle/st-36.html

Netcraft's Web Server Growth
www.netcraft.co.uk/survey/

Network Wizard's Internet grow statistics
www.nw.com/zone/WWW/top.html

NUA's Internet Survey Summary
www.nua.ie/surveys/

U.S. Department of Commerce. "The Emerging Digital Economy II."
www.ecommerce.gov

U.S. Department of Commerce, National Telecommunications and Information Administration's National Internet Usage statistics
www.ntia.doc.gov/ntiahome/fttn99/InternetUse_II/Chart-II-1.html

DIGITAL DIVIDE

Digital Divide (Education Week)
www.edweek.org/context/topics/digital.htm

U.S. Department of Commerce, National Telecommunications and Information Administration.
http://digitaldivide.gov/

Virginia Digital Opportunities Task Force
www.sotech.state.va.us/digop.htm

LEGAL SITES

American Bar Association
www.abanet.org/scitech/home.html

McBride Baker & Coles Summary of E-Commerce and Digital Signature Legislation
www.mbc.com/ds_sum.html

Internet Engineering Taskforce PKIX Working Group
www.ietf.org/html.charters/pkix-charter.html

Internet Law and Policy Forum. “Survey of International Electronic and Digital Signature Initiatives.”
http://www.ilpf.org/digsig/survey.htm

STANDARDS

Extensible Mark-up Language (XML) Signature
http://www.w3.org/Signature/

Government of Canada Public-Key Infrastructure
www.cse-cst.gc.ca/

The LDAP Extension Working Group charter
www.ietf.org/html.charters/ldapext-charter.html

MasterCard/VISA Secure Electronic Transaction
www.setco.org

Minimum Interoperability Specifications for PKI Components, NIST Special Publication 800-15
http://csrc.nist.gov/pki/mispc/welcome.html

“SDSI—A Simple Distributed Security Infrastructure.”
http://theory.lcs.mit.edu/~cis/sdsi.html

The Secure Network Time Protocol Charter
www.ietf.org/html-charters/stime-charter.html

The Simple Public Key Infrastructure Charter
www.ietf.org/html.charters/spki-charter.html

United States Federal Public-Key Infrastructure
http://csrc.nist.gov/pki

STANDARDS BODIES

Accredited Standards Committee X9/American Bankers Association
http://www.x9.org/

American National Standards Institute (ANSI)
http://www.ansi.org/

International Electrotechnical Commission (IEC)
www.iec.ch

International Standards Organization (ISO)
www.iso.ch

International Telecommunications Union (ITU)
www.itu.int

Internet Engineering Task Force (IETF)
www.ietf.org

National Institute of Standards and Technology (NIST)
www.nist.gov

TC68/ISO International Technical Standards Committee for the Financial Services Industry
http://www.tc68.org/

VIRGINIA STATE GOVERNMENT

Secretary of Technology Legislation
http://www.sotech.state.va.us/legis.htm

Council on Technology Services
http://www.sotech.state.va.us/cots/

Digital Signature Initiative Work Group
http://www.sotech.state.va.us/cots/dsi/index.htm

"Toward the Use of Digital Signatures in the Commonwealth of Virginia", (Prepared by the Privacy, Security & Access Work Group, October, 1999)
http://www.sotech.state.va.us/cots/pubs/digsig.pdf

Summary of Electronic Commerce and Digital Signature Legislation in Virginia
http://www.mbc.com/ecommerce/legis/virginia.html#2000%20VA%20HB%20499

Electronic Government Implementation Division
http://www.egov.state.va.us

Executive Order 51
http://www.state.va.us/governor/eorder/eorder51.htm

Executive Order 65
http://www.state.va.us/governor/eorder/eorder65.htm

Executive Order 66
http://www.state.va.us/governor/eorder/eorder66.htm

FEDERAL GOVERNMENT

The Evolving Federal Public Key Infrastructure
http://www.gits-sec.treas.gov/documents/PKI_Brochure.pdf

Federal Public Key Infrastructure Steering Committee
http://www.gits-sec.treas.gov/

The Electronic Signatures in Global and National Commerce Act (An explanation of the Federal E-signature legislation)
http://www.whitehouse.gov/WH/New/html/20000630.html

Federal E-signature Legislation
http://www.mbc.com/ecommerce/legis/106_2d_sess.htm

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
http://www.hcfa.gov/regs/hipaacer.htm

Access Certificates for Electronic Services (ACES)
http://www.gsa.gov/aces/

Electronic Commerce Policy
http://www.ecommerce.gov/

OTHER STATE GOVERNMENTS

California Digital Signature Regulations
http://www.ss.ca.gov/digsig/digsig.htm

Georgia Digital Signature Task Force
http://www.cc.emory.edu/BUSINESS/gds.html

Indiana Digital Signature Information Page
http://www.ai.org/digitalsignatures/index.html

Kentucky and Electronic Signatures
http://www.state.ky.us/agencies/elecsig/index.html

Maryland Digital Signature Pilot Program
http://www.sos.state.md.us/sos/digsig/html/digsig.html

Massachusetts' PKI Page
http://www.magnet.state.ma.us/itd/legal/pki.htm

Minnesota and Digital Signatures
http://www.sos.state.mn.us/business/digital/digsig.html

Nebraska Digital Signature Act
http://www.nol.org/home/SOS/digitalsig/digsig.htm

New York Electronic Signatures and Records Act
http://www.irm.state.ny.us/esra/esra.htm

North Carolina Electronic Commerce Work Group
http://irmc.state.nc.us/ecwg/

Texas Electronic Government
http://www.state.tx.us/EC/

Utah and Digital Signatures
http://www.cio.state.ut.us/399/digsigindex.htm

Vermont and Digital Signatures
http://www.state.vt.us/psd/teledigisig.htm

Washington State and Digital Signatures
http://www.secstate.wa.gov/ea/default.htm

Wisconsin and the Commission on the use of Electronic Signatures
http://www.esignatures.org/

INTERNATIONAL PKI AND E-COMMERCE

Argentina Digital Signature Law
http://www.cnv.gov.ar/English/FirmasDig/

Australia's Attorney General's E-commerce Homepage
http://law.gov.au/publications/ecommerce/

Canadian Government
http://www.cio-dpi.gc.ca/pki/Documents/documents_e.html

Danish Government IT Security Council
http://www.fsk.dk/cgi-bin/left-org-commite.cgi?doc_id=3565&doc_type=488

European Commission
http://www.ispo.cec.be/eif/policy/97503toc.html

France in the Information Society
http://www.internet.gouv.fr/francais/index.html

German Digital Signature Laws and Ordinances
http://www.kuner.com/

Irish Government E-commerce
http://www.irlgov.ie/tec/communications/society.htm

Italian Government E-commerce
http://www.aipa.it/

Singapore's Controller of Certificate Authorities
http://www.cca.gov.sg/

ORGANIZATIONS

National Electronic Commerce Coordinating Council
http://www.ec3.org/

The PKI Forum
http://www.pkiforum.org/

The American Institute of Certified Public Accountants
http://www.aicpa.org/

Internet Engineering Task Force: PKI Working Group
http://www.ietf.org/html.charters/pkix-charter.html

Internet Law and Policy Forum
http://www.ilpf.org/

Interworking Public Key Certification Infrastructure for Commerce, Administration, and Research
http://ice-car.darmstadt.gmd.de/

Section of Science and Technology – American Bar Association
http://www.abanet.org/scitech/ec/isc/home.html

The Federal Electronic Commerce Program Office
http://www.ec.fed.gov/

MISCELLANEOUS LINKS

The PKI Page
http://www.pca.dfn.de/dfnpca/pki-links.html

Electronic Privacy Information Center: Digital Signatures
http://www.epic.org/crypto/dss/

CIT PKI Group: General PKI Help
http://www.alw.nih.gov/PKI/general-refs.html

Digital Signature Guidelines Tutorial
http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

Electronic Commerce Center
http://www.lawdesk.com/ElectronicCommerce.htm

APPENDIX F

STATE AUDIT SURVEY SUMMARY

Prepared for the Audit & Assurance Team
June 9, 2000

In May of this year a nationwide survey of twenty-three states was conducted. The purpose of this survey was to gather information of specific interest to the DSI auditors forming recommendations on decision model criteria and an audit control framework. States contacted were those purported to have digital signatures or PKI infrastructures in place, RFPs issued, or those with enacted digital signature legislation. The following primary questions were targeted with additional information gathered as time permitted:

- Describe the audit program that has been established for your PKI. Is it internally or externally conducted? What is the audit cycle? What are the objectives?
- Was there auditor involvement in the development of your PKI? Is there an audit report that has been issued?
- For agencies and other organizations using digital signatures, do you have specific criteria for when digital signatures would/would not be used? What are these criteria and associated rationale? What are any operational or cost implications for the criteria that have been adopted? Were these guidelines established by statute, Executive Order, Administrative Authority, or by some other means?
- Are there other standards and guidelines for use of digital signatures?

AUDIT CONTROL FRAMEWORK DEVELOPMENT

Generally speaking, auditors from other states have had limited if any involvement in the investigation and development of the audit component for their PKI infrastructure. States that appeared to have the most auditor involvement were Illinois, Washington, Oregon, Kansas, and North Carolina. Although many others viewed this preliminary involvement as beneficial, they did not commit resources on the front end to address any concerns that may arise as a result of implementation.

Additional information provided by various states focused on the types of Certificate Authority audits conducted. As examples, California requires a SAS70 audit, and Washington requires a CS2 audit.

DECISION MODEL CRITERIA

Information on establishing a decision model for determining when or when not to use digital signatures was a bit more specific although guidance is still in its infancy. Several states have determined uses for digital signatures in some form, but no states have firmly established a formal level of guidance in evaluating the usefulness of digital signatures. The overriding commentary did indicate, however, that an evaluation needed to be conducted on an application-by-application basis. Utah, for instance, has formed a Policy Authority to conduct such an evaluation. The following are general, but not necessarily formal guidelines from states on when or how to use digital signatures:

- A need to tie a signature to a document must exist and/or a need to establish non-repudiation must exist.
- If notarization is required then digital signatures cannot be used.
- It should be tied to issues dealing with legal standing or significant monetary implications
- If a government (state or local) signature is required (by statute, administrative rule, court rule, or OFM policy) on official public business with electronic records (a record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another) than digital signatures are required using licensed certificates (State of Washington, RCW Chapter 19.34).
- Business process owner establishes whether or not to use a digital signature. Consider the least intrusive method such as a PIN over a digital signature.

APPENDIX F

ADDITIONAL ISSUES

In investigating decision model criteria and audit control frameworks many other points of interest were mentioned. The range of topics covered access control mechanisms, DMV as a Registration Authority, issuing single certificates only, and the state serving as the central Certificate Authority to name a few. Listed below is commentary received or questions posed that may be addressed by states at a later date.

- If the DMV serves as the Registration Authority several issues need to be considered: general citizenry will have privacy issues, and to avoid such privacy issues consider its use for government/public documents only (Certificates would need to indicate said purpose)
- The state serving as a Certificate Authority would be cost prohibitive
- Individual agencies are serving as their own RA
- Access control mechanisms should be either in the application or in a policy server (policy server considered to be the better option)
- Certificates will contain various authorization levels that allow access rights to file taxes and documents but may not be allowed to handle other transactions online
- Digital Signatures may not be necessary for many transactions—a PIN and/or password may prove sufficient
- Need to address whether or not a uniform identity authentication standard is needed.
- Normalizing the RA process would most likely involve turning it over to the CA to ensure it is conducted in a consistent manner. Another way to normalize the process is to issue single certificates with only one level of assurance.
- The decision to outsource the CA function is twofold: technology is changing rapidly, and the state’s regulatory office is cabinet level containing elected officials
- Looking into the state’s Human Resources department as the RA for agencies, and the DMV as RA for business and citizens.
- When applications are developed that involve citizen interaction the CA will be instrumental in conducting citizen education.

STATE	CONTACT	AUDIT INVOLVEMENT	COMMENTS
Alabama	Peggi Douglas and Gene Akers	No	Not aware of any agency that is currently working on the project. They have had a house bill (#730) that deals with the legality of d/sign but not the implementation.
Alaska	Jay Druvenstein		
Arkansas	Mike Kemp		
California	Lee Kercher 916-445-3220 Alfie Charles (Office of Secretary of State) 916-653-6575	None in development process. Deloitte & Touche audits CAs before they are accepted to do business with California—SAS70	Implementation in California is not yet happening. There are no business processes built yet by agencies. This is mainly because of the way CAs "bind" the digital signature within the Certificate Policy (it is not set up for high government standards). In Government to Government (G 2 G) transactions, not everyone has access to a PC. They may gravitate to biometrics through Signature Dynamics. **Digital Signature Guidelines:** Have to have need to tie a signature to a document. Have a need to establish non-repudiation. **Thoughts on DMV serving as RA:** Too many mitigating factors if applying to general citizenry such as privacy issues. Does DMV really have appropriate level of technology? If just serving as RA for government/public documents this may work—the certificates would indicate for "public documents only". The state serving as the CA would be too cost prohibitive. **Legislation/Regulations:** Both parties have to agree it would be a binding signature. http://www.ss.ca.gov/digsig/regulations.htm
Florida	Charles Ghini 850-922-7439	No	Passing some legislation now. He is just beginning to investigate the use of digital signature in Florida. Denise Potvin may have more information on legislation
Georgia	Steve Akridge 404-657-0818 sakridge@doas.state.ga.us	None to date	Looking at developing a scaleable PKI model for the state. 77 agencies in Georgia—each operated independently. Department of Administrative Services (Steve Akridge) is only department looking at PKI now. They will be the CA within their own department only. Would imagine several CAs would have to exist in the state since there are 100,000 state employees.
Hawaii	Wayne Horie 808-586-0600	Not sure	They are only beginning to look at whether or not to pilot. Have passed legislation (have a hard copy).

STATE	CONTACT	AUDIT INVOLVEMENT	COMMENTS
Illinois	Brent Crossland 217-557-4063	Comptroller's Office	Per news article: Signed an enterprise-wide agreement with Entrust to secure both internal transactions and for transactions with businesses and citizens. They are finalizing plans to launch a pilot. State will operate its own CA and issue one certificate to citizens containing the various authorization levels based on the ways a person might communicate with the government—but there are many policy details to work out before rolling out a production PKI in June. Another policy question to address is whether a uniform authentication standard is needed. Illinois is in the process of statewide PKI implementation. They from the very beginning approached the effort not so much from a pilot perspective, but as if it was going enterprise wide. Their CA will go up in the next couple of weeks and will be the Department of Central Management Services for state employees (root CA). Any other agencies that wish to establish their own CAs must remain subordinate to the root CA and certified by the Secretary of State. He indicated that the root CA would be providing any cross certifications necessary. The DMV, as part of the Secretary of State, will be or is considering the RA function for citizens. They are also considering a larger agency to handle the RA function for large organizations doing business with Illinois. There are still no established guidelines on when or when not to use a digital signature — he said it's still a gray area but imagines it would be tied to anything with significant monetary or legal standing. They have had auditors involved in the process, specifically the comptroller's office. They had a vested interest in their payment processes. The Department of Revenue has also been involved. Their Attorney General and Auditor General prefer NOT to be involved until AFTER the policies have been drafted.
Iowa	Ken Adrian 515-281-7037 ken.adrian@its.state.ia.us	No	Just awarded contract to Baltimore Technologies to do a baseline assessment of trust requirements. They will go to 20 agencies, develop CONOPS, PKI needs (basic trust needs, and CP/CPS), and do a cost evaluation of CA and RA. It is due June 30th. Per news article: Has not decided if the state will operate its own CA or allow a third party. They have determined that they will use single CA certificates. The certificates will contain various authorization levels that allow access rights to file taxes and documents with the secretary's office but may not be allowed to handle other transactions online. One likely scenario on how to issue digital certificates to citizens would be when renewing their driver's license. Digital signatures may not be necessary for many transactions—maybe PINs and a password will be sufficient. Would like to see open standards PKIX so certificates can be interoperable. Legislation: House Bill 2205 www.state.ia.us/government/its
Kansas	Debra Lowling-Chair of D/sign committee 785-296-5275	Yes- Debra is researching who we should contact	Passed UETA in March with an "ABA" (American Bar Association) twist. Currently developing an RFP to get a CA for the state. She hopes that this will encourage agencies to go through this CA instead branching out on their own. In turn, she hopes that this will leverage the CA to reduce the price of Certifications.

STATE	CONTACT	AUDIT INVOLVEMENT	COMMENTS
Louisiana	Chris LaBlanc and Allen Doescher 225-342-7105	No	Within next two months looking to get a workgroup together. Does have legislation passed. He would be the workgroup lead when they do start something.
Massachusetts	Claudia Boldman 617-973-0857	No "We {Technology Department} develop policy and the auditors audit against it. They aren't interested in policy-making, however our Comptroller is very interested."	No legislation has been passed for digital signature. They have their own UETA in draft form, but are waiting for federal bill to come about for specific wording. They have had two pilots (getting their feet wet) : • Government to banking pilot. 20 banks were involved, they used Entrust certificates. Was a disaster for the most part. She indicated that there was not support for end users and software installation had no support. Pilot was not well documented. • Took part in the multi-state e-mall (i.e.: Extranet Email purchasing) pilot. They followed the OBS purchase system. Used donated certificates by Motorola. As before, the technology was fine and on target, but their software applications proved to be problematic. Support issues on users side. Again, even though this pilot ran for a year, it wasn't successful and they shut it down. Although Massachusetts sees benefit in digital signature they aren't real confident and are waiting to see what others are going do. Haven't gotten their arms around how it all "works" such as issuing and revoking. She said, "We are taking a cautious attitude. There are too many trust issues not resolved". Admitted that when they try again, it would be aimed at business not citizens for a while. Their CIO of Technology (David Lewis) used to be CIO of DMV and is interested in the DMV acting as an RA. His contact information is 617-973-0735 and email is david.lewis@state.ma.us
Mississippi	Clay Kiddler-601-359-1685	None currently Did admit to seeing benefit.	Law passed in 1997: Digital Signatures Act. They currently have no demonstrations or pilots running at this time. They have no acting RA, no entities that they are certifying, and they are going to use UETA to remove the cryptography clause. Two planned demos are as follows: • Secretary of State: 3 month run time, dealing with campaign finance reports. Would be using Microsoft Windows 2000/PKI to issue certificates-all in-house. • E-government Initiative Group will make a proposal for an Enterprise-wide digital plan for government. Will run demonstration off of recommendation. Looking to use the Human Resources Group as an RA for agency level staff and the DMV for private and government business and citizens. Looking to charge a CRL fee based on usage. They see a selling revenue potential based on classification of the cert. Believes banks will bring in the largest revenue.

STATE	CONTACT	AUDIT INVOLVEMENT	COMMENTS
New Jersey	Don Johnson 609-633-8919	No, but need to. Claims there is a "raging" debate at the federal level on whether or not to use.	VeriSign is their CA (but later in conversation he said several agencies serve as their own CAs). Each dept serves as its own RA. Used PKIX4 to develop CP/CPS. Department of Labor is going into production with a workers compensation application this summer—even without legislation enacted. The group involves all lawyers using it for authentication only to their database. Access Control Mechanisms should be either in the application, or in a policy server (policy server is better option). They determine digital signature Guidelines on a per application basis. They use three levels of security (see VeriSign) and are developing a CP/CPS for each level—this may lead to digital signature Guidelines or maybe it is only to articulate the difference in RA processes. He sees the necessity of using a level 3. Says there is no legislation specific to digital certificates. **Business Case:** we must do secure business over the internet and can't do it out of band so has to be as secure a transmission as possible and have to know who it is coming from. Then you have to decide if you want to do this yourself or outsource it.
New York	Julie Leeper	None currently.	Following federal bill. Looking at a central statewide initiative. Agencies are currently getting started. Auditing process on web site. A single pin number won't meet New York standards, need to use a combination of biometrics, currently working out these details.
North Carolina	Greg Kreizman 919-850-2729	Audit department involved as a pilot. They are testing confidentiality. Contact is Martin Vernon 919-807-7500 martin_vernon@ncauditor.net	North Carolina's E-commerce Act and E-commerce Rules — CP 12/31/99 are located at: http://www.secretary.state.nc.us/ecomm/ecrules.htm In the E-commerce Act the only guidelines for digital signature were, if notarization is required, then you cannot use e-signatures; all public agencies may accept e-signatures. Have not passed UETA. They will be testing only one software solution for pilots (vendor will write the CP/CPS). The five pilots will test encryption and digital signature.

STATE	CONTACT	AUDIT INVOLVEMENT	COMMENTS
Oregon	Pat Lundene 503-378-6029	Internal Auditor: Valerie Wicklund 503-378-3742 Secretary of State Auditor: Neil Weatherspoon 503-986-2255 Sub-Committee on Security Standards: Phyllis Michael 503-378-5917	Passed digital signature legislation in 1997 No set usage guidelines other than the Business Process Owner establishes whether or not to use a digital signature. They believe the least intrusive method should be used—for instance, if a PIN is sufficient, then a digital signature should not be required. One "for instance" was that if they knew the person they were dealing with then maybe only a PIN would be required—this could be considered a guideline of sorts. Other than intra-governmental operations ("server-to-server") there are not any applications in place that have necessitated a certificate. When applications are developed that involve citizen interaction they will hire a national CA mainly because they will conduct the citizen education portion in a much more comprehensive manner than the state could. They have been working on DIGITAL SIGNATURE for 18 months with nine statewide committees to establish the issues with PKI, propose recommendations on an enterprise strategy. Their 125 agencies are all very autonomous, so an enterprise strategy may be difficult.
Pennsylvania	Rhett Hintze 717-705-0350.		Passed UETA- Reference copy of their IT Bulletin.
Rhode Island	Sally 734-5141		
South Carolina	Ruth Kirtland and Jimmy Earley 803-896-7890	None currently	In the IT department there is no legislation for digital signature. DMV is capturing digital signature on driver's license currently. (Note: There has been issue about the DMV selling the images — argument that it lacks correct privacy controls). They are in the process of setting up a committee in the Budget Control Board and Information Resources Council to look at D/sign. He sees the DMV being the RA for individuals and the Budget and Control Board being the RA for Businesses. Is willing to discuss with us.
South Dakota	Otto Doll 605-773-3416 Jan Newman 605-773-6971		UETA passed, nothing else has been started as of this time. Jan Newman would be the chair of a workgroup/committee when formed.
Utah	Robert Stewart 801-538-1862	None involved in development process External auditors conduct audits of CAs.	A Policy Authority comprised of a number of individuals determines whether or not an application warrants the use of digital signature. It is evaluated on a case-by-case basis; no general guidelines have been established. International standards (IETF) were followed when developing CP. Four licensed CAs in Utah. SB 761 could effect electronic signature legislation.

STATE	CONTACT	AUDIT INVOLVEMENT	COMMENTS
Washington	Scott Bream 360-902-3460 scott@dis.wa.gov	Mike Ricchio, Secretary of State's Office 360-753-2896 (Involved in Task Force that was assembled to decide which type of audit would be conducted on CAs—CS2). He will be able to provide rationale for decision.	**Per news article:** Digital Signature Trust Co will issue and manage digital certificates for businesses and citizens. The company will help state officials write policies for its PKI and create applications. Citizens will obtain certificates by downloading a form from a www site, having it notarized at a bank and submitting it to the company. In addition, several state agencies will issue certificates. First, the state will tackle creating access control mechanisms for transactions over the Web, such as filing taxes electronically. And state agencies will begin to sign forms using a digital signature capability. Washington will launch a campaign to educate people about how digital signatures work and how to protect their certificates. **Conversation with Scott Bream:** Electronic Authorization Act 19.34 prescribes the manner in which a CA operates and the behavior of the subscriber, and the processes that are sufficient to establish a trustworthy system. If the CA follows all the prescribed procedures, the presumption of law gives the benefit to the CAs and the defense has to prove otherwise. The subscriber also gets the benefit of law in the validity of their signature. The law is silent on access control issues. The decision to outsource the CA function was twofold: technology is changing rapidly, and their regulatory office is cabinet level containing elected officials. The RA function is still handled internally, however, which is an issue. In order to control the accuracy of authentication, they would like to "normalize" the RA process as much as possible. Currently different agencies may be authenticating at different levels that may not provide the security the State is looking for (the CA also refuses to take responsibility for any issues that arise due to authentication procedures since they are not involved). Therefore, they will more than likely turn the RA function over to the CA and have them develop a process that is accessible (via banks and notaries, for instance) yet one that they (the CA) are totally responsible for. Another factor in normalizing the RA process is to issue single certificates only. This way the highest level you need would be issued, vs. issuing different certificates for different levels of authorization. Access would still remain at the application level vs. contained in the certificates. They have not determined which applications would require high, medium, or low authorization levels. **Decision Model/Usage Guidelines:** The only place that gives any sort of description of when to use a digital signature is in their AGOs interpretation of EAA 19.34 which says: when it is required by law that a handwritten signature be applied, then a digital signature fulfills the same requirement if the certificate has been issued in accordance with the law.* They could not determine what types of criteria (such as high $$$ transactions, leave slips, etc.) would require certain types of signatures and they have not wanted to set a precedent.

APPENDIX G

DSI DEMONSTRATION PROJECTS

SEPTEMBER 19, 2000

	BUSINESS FUNCTION	PARTNERING ORGANIZATIONS	CERTIFICATION AUTHORITY AND PRODUCT USED	DEMONSTRATION OBJECTIVE
G 2 G	Electronic purchase requests and approval → **Will move to production environment**	**Department of Game and Inland Fisheries**	**CA:** Served as own CA **Product:** Entrust 600 + certificates issued	Demonstrate agency-wide use of digital certificates for requests and approvals of purchases, travel vouchers, and law enforcement reporting forms. Additional use for certificates in the next year are: time accounting submissions, personnel forms, budget change requests and all other administrative paperwork.
	Certification for Funds Transfer: Mobile Home Sales	**DMV** **Fairfax County** **Chesterfield County**	**CA:** VIPNet **Product:** Entrust 16 certificates issued	To evaluate business impact of replacing manual signatures with digital signatures. To evaluate e-mail as a transport mechanism for confidential data. To evaluate the integration of PKI into application software packages.
	Certification for Funds Transfer: Additional Rental Sales Tax	**DMV** **Fairfax County** **Chesterfield County**	**CA:** VIPNet **Product:** Entrust 16 certificates issued	To evaluate business impact of replacing manual signatures with digital signatures. To evaluate e-mail as a transport mechanism for confidential data. To evaluate the integration of PKI into application software packages.
	Information Exchange between State and Local Government Parking Ticket Information	**DMV** • City of Charlottesville	**CA:** VIPNet **Product:** Entrust 8 certificates issued	To evaluate the use of PKI encryption to determine what factors make this viable for a production environment.
	Secure Web-based Electronic Filing of Court Documents → **Will move to production environment**	**Wise County/City of Norton Circuit Court** • Big Stone Gap Housing Authority • Law office of Kern & Kern • Notary Public • Powell Valley National Bank	**CA:** DIT **Product:** VeriSign 5 certificates issued	To enable the filing, searching and retrieval of public Circuit Court land record documents (Deed of Trust) remotely and electronically for all participants.
	Web-enabling state-wide telecommunications request form → **Will move to production environment and to G2G category**	**Department of Information Technology** • DGS • Virginia Employment Commission • Dept. of Conservation and Recreation • DGIF • DMV • Chesterfield City • City of Norfolk	**CA:** VeriSign/DIT **Product:** VeriSign 17 certificates issued	Demonstrate internet e-form which allows state and local agencies to electronically sign and submit telecommunications requests. Electronically update mainframe productions database.

	BUSINESS FUNCTION	PARTNERING ORGANIZATIONS	CERTIFICATION AUTHORITY AND PRODUCT USED	DEMONSTRATION OBJECTIVE
	Electronically Managed Travel Authorization and Reimbursement	**Department of Motor Vehicles** • Unisys Corporation	**CA:** Baltimore Technologies **Product:** UniCERT 38 certificates issued	Demonstrate PKI integration into intranet e-forms including multiple signature authorizations and multiple key storage mechanisms. Identify the integration points required for enterprise architecture.
	Personnel requisition submission and processing **Pilot pending**	**City of Norfolk**	**CA:** DIT **Product:** VeriSign	Demonstrate web-enabled data base application to manage personnel requisitions, using intranet e-form with multiple signatures.
G 2 B	Interagency transfer of funds **Plan to move into production environment** **Pilot pending**	**Virginia Information Providers Network (VIPNet)** • DMV • VIPNet Authority Board • VIPNet Authority Board Executive Committee • Virginia Interactive, LLC • DIT Fiscal staff	**CA:** Served as own CA **Product:** Entrust 10 certificates issued	Use of digital signatures to provide electronic authorization for interagency transfer of funds.
	Electronic bidding for VDOT contracts **Will move to production environment**	**Virginia Department of Transportation** • Virginia Road and Transportation Builders Association • Industry representatives • Federal Highway Administration Representative	**CA:** InfoTech, Inc. **Products:** Expedite, Bid Express 11 certificates issued	Demonstrate electronic distribution of Requests for Proposals (RFP) and electronic submission of bids into a secured system.
	Electronic Procurement	**Department of General Services (DGS)** • Vendors (North Carolina and Massachusetts) • James River Correctional Center Purchasing Department • Division of Purchases & Supply	**CA:** VIPNet **Product:** Entrust 14 certificates issued	To evaluate the use of a managed certification authority and digital signatures in the state procurement process. This was accomplished with a DPS Purchase Requisition form electronically submitted to DGS, digital signature authorization of the form, and “Notice of Award” documents posted on DGS Procurement web site and emailed to suppliers.

GENERAL LESSONS LEARNED

SEPTEMBER 11, 2000

The following “lessons learned” were chosen as they applied to more than one Digital Signature Initiative pilot organization.

1. Involve end users in all phases of planning, testing, and implementation
2. The learning curve is steep, especially with varied levels of computer literacy. On-going education and training is an essential component of a successful implementation. Vendors must be available extended hours to support implementation and maintenance of services.
3. The relationship between clients and vendors is critical. Getting all participants to effectively work together is critical. Vendors and clients must clearly understand each other’s requirements and capabilities or constraints.
4. Review vendor technical requirements well ahead of purchase in order to become aware of potential incompatibility issues.
5. Top-level management should be involved from very beginning to understand the high-level of organizational and resource commitment required to implement and support PKI.
6. Interdependence between users and systems must be understood by all participants.
7. Applications integration is challenging. Setting up a test environment specific to the application is critical.
8. New and evolving PKI technologies may be ahead of the current policy and legal framework.
9. Digital signatures should only be implemented after all procedure, policy, and application options have been considered. Current business practices and policies may need to undergo a re-engineering effort to handle digital signature methodology while maintaining the same level of controls and protection.
10. Need to retain digital signature public keys and revocation lists at the same retention schedule as the document
11. Electronic forms requirements initiate review of current agency policy and possible re-engineering of processes
12. Using a forms package requires that each user has the package. Data extraction from forms is complex and requires field-level programming.
13. Authentication processes could be facilitated by having more Registration Authorities, especially when users are remotely located.
14. By keeping authorization at the application level, rather than embedding authorization information in the certificates, modifications of authorizations can be accomplished without reissuing certificates.
15. For cross-certification purposes, the URL for the remote CA would need to be listed in the certificate. The remote CA’s CRL must be located outside their private network/firewall to allow access to other users for verification purposes.
16. Encrypting and digitally signing documents requires individual keystrokes that cannot be done at the server level. Therefore, signing and encrypting are not recommended for large production level use.
17. Consider the level of security and application requirements as critical factors in selecting key generation methods and storage media.
18. Electronic forms should be accessible from a Web-Server to provide a central point for access and a single point for version management. The form should be distributed through a browser. This substantially reduces the overhead required to manage form releases and updates to the desktop.
19. The installed E-form product should provide the ability to digitally sign the server-based form without being restricted to a specific PKI vendor. It should be able to use the signing key regardless of whether it is stored in the browser, client software, or hardware token. It should support the signing of individual fields or the whole document, multiple signatures and archival of the form along with the contents.
20. While E-form packages have developed substantial interoperability with PKI structures and to back-end databases, they do not interoperate with each other. A form developed with one vendor’s software does not function in another vendor’s environment.

GENERAL CONCLUSIONS DRAWN

SEPTEMBER 11, 2000

1. The reengineering of processes must proceed decision to implement PKI
2. Certificates will not be ubiquitous for several years
3. PINS, passwords, tokens, etc. will coexist over next several years, but digital signatures will be dominant in the end
4. Education, with emphasis at the user level, is essential.

PILOT	VENDOR, PARTNER ORGS. & CERTIFICATE AUTHORITY RELATIONSHIPS	SOFTWARE/HARDWARE	AUTHORIZATIONS/ACCESS	SIGNING/ENCRYPTION	SECURITY
DMV/Tax	Partner organizations must understand administrative processes and workflows before transactions begin. Support from the CA/RA is not available outside business hours for problems. Support during all business hours will be critical to continuity of business operations. Suggest 24x7 support. Training sessions needed to address how PKI is to be used generally and specifically. User guide needed that covers install, use of multiple machines, removal, and how to configure the interface with various application packages.	Update to user desktop client necessary in order to install Entrust client. Changes to routers as well as firewall necessary for communication to be enabled. After installing desktop client an icon went into system tray. After rebooting system the Icon disappeared. If user works on more than one desktop, a different certificate is required for each. Can cause confusion for receivers of data. Entrust requires specific releases of email clients. Email has configuration issues that are not intuitive to the user: to find certs for email recipients a setup process is required, use of PKCS7 encoding disrupted the handling of Internet (external) email address, and sending material to more than three users causes an error in handling the internet addressing for the third user. Even without email integration the mail item can be drag/drop to the desktop and managed outside of	The movement of the credentials from one PC to another is not a developed process. The variations of activity with the client software need to be fleshed out so they can be handled consistently: unlock password, restore credentials, reinstall client, and how to have this on multiple desktops?	The PKI architecture implemented does not allow the signing/encryption to be done at a server level, and requires manual intervention for every dataset to be sent out. This restricts the use of PKI for large production level use. Difficult to determine who sent an encrypted file that is not signed—Entrust client does not indicate sender. Could end up opening a potential virus without knowing who sent it. PKI enables transport of confidential data via email. Things to consider, however, are: encryption and signing are manual functions (therefore not recommended for high volume transactions), data must go as an attachment so as not to lose format, and going from a paper-based to an electronic forms-based system requires re-engineering of policies regarding data changes (i.e. How does the final signor know what data the original signor may have submitted?) There is a margin of casual error in remembering to activate/deactivate the signing or encryption process. You may end up signing and encrypting more often than required (or vice-	To setup the needed network infrastructure, open as few ports as possible and, perhaps, not some of those recommended by the CA. Need to ensure that both passwords for initial sign-on to the system are kept out of any one person's hands.

PILOT	VENDOR, PARTNER ORGS. & CERTIFICATE AUTHORITY RELATIONSHIPS	SOFTWARE/HARDWARE	AUTHORIZATIONS/ACCESS	SIGNING/ENCRYPTION	SECURITY
		the email client. Mainframe-centric systems do not convert cleanly to a PC based environment. Generating mainframe output into email invites critical data being dropped from records. No alteration of mainframe data is tolerated.		versa) unless you specifically remember to deactivate the function. Since the actual signing and encryption of the document takes place behind the scenes and the sender does not view it, how do you know this has actually taken place. When sending a clear text message that has been digitally signed in Entrust to a receiver without Entrust, the receiver can read/view the text message, but not open it. While it is possible to find and view the contents of the message, it has to be done through non-standard handling such as "view" rather than "open". The appearance of the message will also contain extraneous characters.	
Wise	Policy and procedures are more important than technology issues—all partners should work together from the very beginning. Most existing policies and procedures are not sufficient to allow the implementation of electronic signatures. If the legal framework is not willing to adapt to the new document solutions, the benefits will not take place as fast as they could.				

PILOT	VENDOR, PARTNER ORGS. & CERTIFICATE AUTHORITY RELATIONSHIPS	SOFTWARE/HARDWARE	AUTHORIZATIONS/ACCESS	SIGNING/ENCRYPTION	SECURITY
DIT	A complete workflow requirements document should be one of the first steps taken. Define all current process inputs and all outputs down to a detailed level. A detailed requirements document is essential to provide vendors a roadmap to accomplish their tasks. Vendors should be onsite during installation and testing to quickly resolve issues. Perform a business/risk analysis before implementation. Forms vendors need to deliver sufficient documentation on supporting the form and how to modify it to fit particular needs. Invite users to participate in e-form design. Users prefer to be stepped through the registration and usage process versus following online instructions. Need to have: design requirement, a test database, a long-term test database, input from users on form design, and form format. Getting vendors to work together effectively is paramount. After delivery of products, vendors should still have a commitment to success of the environment.	Packages to transport data from e-forms to database require different interfaces. In some instances no further development was needed, in others it was. There were issues in setting up the Secure Server. The main issue to resolve was the validator which could be attributed to learning new technology or the installation documentation wasn't clear. The validator on any connection to the Web server creates the SSL connection to validate the certificate by checking the CRL. Using the validator in this fashion is not how it would be used in a production environment with many users. Setting up a test environment specific to the application is critical. Require satisfactory amount of user testing before rollout.	Not enough activity to keep the SAGA Broker software from timing out. Authentication process to register users is difficult without further deploying additional RAs, especially when users are remotely located. Certified mail is a slow process. Showing proper identification for remote users must be accommodated, as well as delivery of passwords. Investigate production files that may be password protected and incorporate this into requirements definition.	Browsers must be tested for ability to handle signing.	

PILOT	VENDOR, PARTNER ORGS. & CERTIFICATE AUTHORITY RELATIONSHIPS	SOFTWARE/HARDWARE	AUTHORIZATIONS/ACCESS	SIGNING/ENCRYPTION	SECURITY
	Suggest reference checks of vendors to determine quality of product and service delivery. Users must know how to move their certificates from one machine to another if the need arises.				
Norfolk	Need to review vendors' technical requirements well ahead of purchase of a particular solution in order to be aware of potential incompatibility issues. Top management should be involved from the beginning to understand the high-level of organizational and resource commitment needed to implement and support PKI. PKI has both a large technical component and a large business component that requires policy administrators, legal consultants, project managers, programmers, functional users and computer network specialists to implement. Investigate and compare vendor products and services as they relate to specific needs. The right mix of internal skill sets needs to work on implementation due to its large technical and business components.	Entrust solution for CA access is not compatible for use with proxy server or SOCKS proxy. Software uses a hard-coded IP address in its compilation that further hinders efforts to use IP translation methods for proxy usage. Workaround option not viable.			

PILOT	VENDOR, PARTNER ORGS. & CERTIFICATE AUTHORITY RELATIONSHIPS	SOFTWARE/HARDWARE	AUTHORIZATIONS/ACCESS	SIGNING/ENCRYPTION	SECURITY
Fairfax	Capabilities of various vendors to support PKI and digital signatures as well as vendor-specific solutions must be investigated thoroughly. Internal processes of partner organizations need to be detailed. Support from CA and partner organizations for administrative and technical processes is critical.	Difficulties in establishing TCP connection with CA. All ports on both sides were opened; perhaps router is blocked. More details needed on how product works and characteristics, and protective measures necessary. Access through firewall was initially difficult. Need to understand necessary rules. Actions such as replacing desktop platforms, updating software, or changing the network configuration can cause the certificate to no longer function properly.	Certificate download and usage instructions need to be more specific. Much had to be learned through experimentation.		Current business practices and policies must be modified to handle digital signature methodology while still maintaining the same level of controls and protection.
Chester-field		Additional safeguards may need to be in place for laptop computers with digital signature software.	Must be able to permit access to public documents under FOIA.	Experience font format issues when importing encrypted data within a mail window (not an attachment) to a Word document. Some formatting was lost and margins and tabbed fields appeared askew. If document is received as a Word attachment the formatting of the document is successful and all the field entries printed correctly.	Security safeguards for confidentiality of dial-up laptops that have digital signature capability software.
UVA	All partners need to plan (in advance of PKI purchase) to ensure policies' capacities to participate in cross-certification through the Bridge. Users and decision makers don't want to and don't need to know everything about PKI technology. They just need to have confidence that it works to provide sufficient security for the transactions it	Client software and applications do not, yet, have the logic embedded in them to do cross-certification (generally speaking). Keeping the PKI as simple as possible is critical to statewide rollout, therefore, Bridge should only (initially) map the highest-level assurance certificates from participating CAs. Microsoft IE and Netscape employ very different mechanisms for	By keeping authorization at the application level, rather than embedding authorization information in the certificates, modifications of authorizations can be accomplished without reissuing certificates. In the case of vendor solutions that charge based upon the number of certificates issued, there		

PILOT	VENDOR, PARTNER ORGS. & CERTIFICATE AUTHORITY RELATIONSHIPS	SOFTWARE/HARDWARE	AUTHORIZATIONS/ACCESS	SIGNING/ENCRYPTION	SECURITY
	is designed to assist.	signing web-based forms.	should be tangible cost savings realized with this approach.		
VDOT	Allowing initial diskette submission of bids is critical in preparing the contractors for the internet submission. To avoid unnecessary delays all stakeholders must communicate effectively—coordination is essential. User learning curve is steep. Very detailed step-by-step training must take place for acceptable performance.	Server capacity problems initially. Custom application did not interface with partner software until change requests were processed. If changes are necessary to established applications, test changes through incremental steps rather than making one overall change.			
DGIF		Printing in text box of Shana forms requires minimum 10 pt. font size. If less than 10 pt. information doesn't wrap properly and goes outside margins. This was tested on many different models of HP printers with different occurrences at different printers. Do not know if this issue is specific to Shana forms only.	For cross-certification purposes, the URL for the remote CA would need to be listed in the certificate. Also, the remote CAs CRL must be located outside their private network/firewall to allow access to other users for verification purposes.		
DGS	Existing contractual or other types of relationships can be used as a basis of trust.	To verify a digital signature the receiver must have digital signature client software installed (for Entrust signed docs). Currently testing to see if the software must be from the same vendor as issued the certificate. Spoke with Entrust about this issue and discovered that it may be possible to validate a signature without software resident on the desktop, but it is a manual, labor intensive process		Since encryption is performed with the recipient's public key, encrypted email cannot be sent to a generic email address. Generic email addresses do not have a specific identity (which is required for issuing a public key). GroupWise requires an enhancement pack to process RSA certificates properly. GroupWise 5.5.1 defaults to digitally sign everything. Must remember to disable when sending to individuals	

PILOT	VENDOR, PARTNER ORGS. & CERTIFICATE AUTHORITY RELATIONSHIPS	SOFTWARE/HARDWARE	AUTHORIZATIONS/ACCESS	SIGNING/ENCRYPTION	SECURITY
		without an audit trail. GroupWise 5.X will not allow a user to open an email message if it has been digitally signed and the user does not have digital signature client software installed. Entrust views network drives as insecure. Saving an Adobe form to a network drive will invalidate the digital signature. Need to test validation of a digitally signed Adobe form if it is sent through email, which requires using a temp directory for opening the document. Signed documents posted on a web site cannot have the signature authenticated via the Adobe reader. Forms package selection is critical to overall costs: Just purchasing an Adobe reader does not allow verification of identity of the signer; it only acknowledges that it was digitally signed. The full-blown package is needed to verify identity of signature and this cost is significantly higher than just a reader. Using a forms package requires each user have the forms package. Data extraction from forms is complex—requires field-level programming in visual basic or java.		who do not have this software.	
DMV/Travel Voucher	Training is a challenge when users have varied levels of computer competence. Interdependencies between users and systems must be understood by all.	Unisys Info Image Workflow Server could not be brought into the DMV network; as a result the Workflow server had to be reconfigured using DMV equipment. Vendors and clients			Consider level of security and application requirements as critical factors in selecting key

PILOT	VENDOR, PARTNER ORGS. & CERTIFICATE AUTHORITY RELATIONSHIPS	SOFTWARE/HARDWARE	AUTHORIZATIONS/ACCESS	SIGNING/ENCRYPTION	SECURITY
		need to understand one another's constraints and software requirements. IT infrastructure issues that surfaced and need to be addressed prior to production implementation include: remote access to the system, deployment over disparate platforms (i.e. Windows '"5, Windows'98, Windows NT), interoperability issues among system components within organization as well as between the organization and other outside entities. DMV firewall rules had to be modified to allow network traffic to occur at the DMV on an outbound and inbound basis in connection with digital certificate requests, email notification of certificate issuance and installation links.			generation methods and storage media (such as smart cards).

*There were several areas where additional lessons learned would be of benefit for future users of this technology: DNS names, remote access, proxy servers, client configurations, software installation and configuration, Novell GroupWise, interoperability, end-user training and requirements.

DNS Names: The DNS name provided for the issuance of the web server certificate did not agree with the DNS name configured for the DMV server. This did not impact the initial loading of the certificate into the web server, but it did invalidate the certificate for use in establishing SSL sessions. The problem was corrected by changing the DNS name back to agree with the distinguished name in the certificate. The lesson learned was that a DNS name of a web server cannot be changed without re-issuing the web server certificate.

Remote Access: The security policy and firewall rules established at the DMV made it impossible for remote users logged into the DMV network to access the Validation Authority at the Unisys COE (Center of Excellence). The problem was identified but not corrected during the Proof of Concept. The lesson learned was that if the network security policy cannot be changed, the Validation Authority would need to be installed on the DMV network for remote access. This is an issue that should be addressed in the design of the PKI.

Proxy Servers: During the initial testing of the application, requests processed by the Validation Authorities were not being returned to the browser. The problem was solved when the DMV network administrator identified that the client had not been configured to take into account the proxy server through which requests to external networks were channeled. The lesson learned was that a thorough understanding of the network architecture was necessary to ensure the accurate configuration of client software's communication parameters.

Client Configurations: It is not possible in most environments to specify more than the minimum configuration of client platforms. Planning for deployment must include the identification of all client and server configurations that might be encountered on production rollout. The participants in the Proof of Concept had workstations running Windows '95, Windows '98, and Windows NT. The hardware configuration also varied, with some machines having available USB or parallel ports and others without. This did not present problems for the users who stored their certificates within their web browsers or the web based application components. It did impact the ability to deploy the peripherals that were provided for demonstrating the use of smartcards, iKey tokens, and biometric authentication. These products are highly dependent on the underlying operating system (OS) and the availability of communication ports. The lesson learned is that when peripherals are used, the exact configuration of the client platform must be known or specified so that the appropriate versions of software and connecting cables are provided to the user.

Software Installation and Configuration: Several client installation or configuration problems were identified and addressed during the Proof of Concept. In one instance, the installation of a single plug-in failed with no notification to the end user causing execution errors. Several workflow users experienced problems when the client workflow configuration options were not properly set. The lesson learned is that the installation and configuration of client software should be simplified for end users. The installation process should bundle all the plug-ins or extensions provided by each of the 3rd party software vendors and ensure that all components have been successfully installed. Configuration parameters that can be included at installation should also be preset by the client software installation program to minimize the complexity of the configuration process.

Novell GroupWise: Virginia DMV utilizes Novell GroupWise as its E-Mail service throughout its agencies. However, this was not identified in early discussions with DMV prior to the development of an E-Mail Robot (essentially a system user that logs into the system and performs specified functions on items as they enter a predetermined queue). Unisys had asked if the system e-mail was MAPI compliant, which GroupWise is, however the robot configured did not function within the GroupWise environment. Testing prior to install was performed in an Exchange Server environment with Outlook. Additionally, DMV later requested a second E-Mail function within the workflow. Activating a second E-Mail function in an already unstable mail environment was marginally successful. Outlook was implemented, which functioned as tested, however was not capable of supporting two "system" users from the single server in our Proof of Concept environment. Several work-arounds were implemented that still did not completely resolve the issues confronted. Subsequently, SMTP was utilized with an Internet account to send items. This functioned with the exception of not automatically clearing the "outbox" of all mail items created. These difficulties were again brought on by the lack of a thorough and formal Requirements Definition Phase being conducted at the beginning of the engagement. InfoImage and its workflow components, including “system users” could have functioned, as DMV required, had the requirement been identified prior to implementation.

Interoperability Issues: One new interoperability issue arose during the Proof of Concept that reinforces the need to work closely with 3rd party software providers in order to ensure that the integrated solution will meet the needs of the business application relying on the PKI.

When a digital signature is applied to a document, and each time the document is opened, the certificate used to create the signature is verified to ensure that it has not expired or been revoked by the issuing Certification Authority. This process is transparent to the end user of the application unless an expired or revoked condition is detected. During the Proof of Concept, it was intended to demonstrate what an auditor would see if a reimbursement request was accurately processed and a certificate used to apply one of the signatures was subsequently revoked or had expired. Ideally, the auditor would see from the error reported that the certificate had been revoked, but that the revocation occurred after the transaction had been appropriately processed. The reason for the revocation (e.g., the employee had left the organization, the certificate was compromised, etc.) as well as the date of the revocation could then be used by the auditor in his analysis of the transaction. Unfortunately, while the new plug-in provided by the validation software vendor successfully determined that the certificate had been revoked, it did not perform in a manner that would enable the auditing of the transaction after a certificate had been revoked. Unisys is addressing this problem with the vendors and it will be resolved shortly to meet the requirements identified for the audit ability of digitally signed documents over time.

End-User Training Issues: Several problems were encountered with the workflow training. The sessions were not comprehensive enough for the users to get a complete understanding of the workflow process. The training materials were lacking in thoroughness. Several end-users felt that the certificate training and the workflow training was not well communicated among the Unisys team. At times the process seemed chaotic to everyone. The Proof of Concept proved the need for extensive, well organized, well documented thorough training sessions for all participants.

Workflow Requirements - The success of electronic workflow is based on the accuracy of the defining current workflow process. This should involve several sessions to review and document the roles and responsibilities of all participants. The electronic workflow process lacked the integrity of the manual process. Many participants received requests from travelers in other administrations, they were not aware of requests waiting for their approval, they were required to manually route requests to approvers because of errors in the workflow process. Several end-users continued to receive errors after submitting their request into workflow. The new electronic workflow routing process should be an exact replica of the manual workflow routing process. This was not the case and if additional time was spent defining the current workflow, many of the routing problems might have been prevented.

PILOT REPORT SUMMARIES

Each of the eleven pilot organizations submitted reports on lessons learned, obstacles encountered, and status updates on a monthly basis. To view the full reports, visit the COTS Digital Signatures Initiative web site at http://www.sotech.state.va.us/cots/ .

For the August reporting period, each pilot demonstration organization provided a detailed narrative that addressed the following two areas:

1. Describe the criteria your organization used to decide which application to pilot. Explain, in narrative form, the production design and workflow, the process users went through to get and use digital certificates (from an user point of view), and the criteria upon which you based your design decisions. Please include information on who was involved in the design process, and which vendors you chose and why (where applicable).

2. Provide a brief summary of the implementation strategy and the steps taken to put the pilot into production. Please include information on policies and procedures, roles and responsibilities, application integration, and time and funds expended.

The following narratives were edited for clarity and consistency by the DSI staff. Following each narrative is a synthesis of the pilot organization's status reports, containing more detailed information on technical requirements, obstacles, functionality, staffing, elements tested, and testing requirements.

DEPARTMENT OF GAME AND INLAND FISHERIES (DGIF)

By Virgil Kopf, Chief Information Officer, Department of Game and Inland Fisheries

PILOT DESIGN

The Department of Game and Inland Fisheries is widely distributed throughout the Commonwealth. The agency has employees in every county of the state. Nearly 50% of the employees do not routinely report to an office to conduct their activities. Many of these employees work out of their home. The only electronic communications for these employees is through the use of electronic mail. The Department had an administrative need to improve the speed of communications, decrease data entry requirements from data collected on various activities, improve the consistency of data collected and processed, assure integrity of data collected and manage the proliferation of electronic versions of forms. After reviewing various options, an electronic form, digital signature solutions was determined to be the most cost effective option.

The purchasing process was used as the pilot example because it was the most mature and impacted the widest spectrum of employees in the agency. Digital signatures were distributed to employees during the process of upgrading computer system operating systems form 'Windows 3.1 to Windows 95 and the installation of Office 97 application suite. The signatures were distributed primarily in person with some remote distribution using the policies and procedures previously provided.

Electronic forms were eventually developed in Shanna Informed. This product was chosen after initial work in another product was determined to not meet the agency's needs. Four different products were evaluated before determining to use the Shanna product. Digital signature services are provided by Entrust. This product was chosen primarily because of supported interoperability between the Shanna informed product and the Novell Netware operating system used on the agency's LANs.

PRE-PRODUCTION

The system was implemented using the agency's standard develop processes. The form development involved the process owner and end users to determine the needed information and the best format to collected the data. The form was tested and piloted within the agency for several months. The development of these processes was done to support changes in the policies and procedures for purchasing within the agency. The purchasing department was responsible for developing and achieving approval of the policies and procedures.

The purchasing application is currently a stand-alone application that does not integrate with other applications. The next phase of this application however, will be integrated into a comprehensive financial package consisting of budget, purchasing, small purchase cards, and vouchering and asset management.

PROJECT SCOPE & OBJECTIVES

The project focused specifically on the Department's implementation of an e-form based process for requesting, approving and placing purchase requests for all goods and services except those utilizing the state small purchase card. The objectives were to provide a mechanism for remote personnel to an efficient process for requesting purchases, route those request for appropriate approvals, and process the request within the purchasing office without having to send paper through the mail or have multi instances of keying information. The timeframe for processing a request was hoped to be shortened to 1-2 days rather than 7-10 days. The system had to insure integrity of the information. This is to be accomplished through the use of the digital signature. The electronic form was used to insure some data quality assurance and enforce business rules regarding the need for specific kinds of information.

EXPECTED BENEFITS

The process will result in significant savings of time for field personnel in processing request for purchases. Savings will be realized in reduced handling of paper, postage, and data entry efforts. Physical storage of records will be reduced. The project is part of a larger financial package development that will take the purchase request information, check the information against the budget, carry charging information through to the voucher payment and request information into the asset tracking system.

BENEFITS OR SAVINGS EXPERIENCED

The use of the e-form and signature has proven to meet the expectation in time savings, increased data integrity and reduction in redundant data entry. The purchasing process itself is still undergoing some modifications to further streamline the process. The data collected from the IPR process is being used for analysis of how the system can be improved. These are issues outside the actual use of the e-form and digital signature.

STAFFING

No staff members were added for this process. Every employee in the agency has received a digital certificate and uses this certificate for purchasing and other internal administrative process. The distribution and maintenance of the digital signature is conducted by the operations staff and primarily involves part time of one employee. Training for employees was conducted as part of a recent system upgrade and specific instructions were provided to those doing purchase requests. The instruction focused primarily on the process of purchasing. Only a limited amount of time was needed for instruction on the form and digital signature. The training was conducted with personnel from IMS and the purchasing office. The electronic form was designed by development staff as one part in the overall development process.

FUNCTIONAL CONTEXT

Digital signatures are now part of the administrative operations of DGIF. Every employee has been issued a certificate. The certificates are utilized in the purchasing process but are also used for travel vouchers, law enforcement reporting forms and will be used for time accounting submissions, personnel forms, budget change requests and all other administrative paperwork within the next year.

APPLICATION ENVIRONMENT

The Department of Game and Inland Fisheries maintains 6 local area networks. These are located in Richmond and the five regional offices throughout the state. These LANs are connected through a frame relay connections to form an agency WAN. The system has a server in each remote location and a multiple servers located in Richmond. At the start of the process, the network operating system was Novell Netware 4.2. During the duration of the study, the system hardware was replaced and the operating system upgraded to Netware 5.1. Regional offices and remote personnel do not directly connect to the WAN. These personnel communicate with the agency through e-mail (GroupWise 5.5). The e-mail connectivity for remote users is provided through asynchronous services maintained in the Richmond office and accessed through an 800 number from the field. All employees in the agency have access to a PC for business use. Over 95% (including part-time personnel) have a PC issued specifically to them. The PC platform is Windows 95 with the Office 97 application suite. The electronic forms package is Shanna Informed. Each PC has a Shanna form-filing client installed. The digital signature application is Entrust. Every employee is issued a digital signature a part of the process of establishing computer rights and computer accounts. Additional hardware was purchased to support the RA and CA components of the Entrust framework. These systems utilize Windows NT 4.5. A software upgrade of the directory utilized to store public certificates and revoke certificate lists was purchase with the intent of supporting the testing of cross certification. This was not utilized in the pilots and would not have been needed for DGIF use.

CERTIFICATE AUTHORITY

Entrust.

LIST OF CERTIFICATES

The agency has issued over 600 certificates to employees of the agency. No certificates were issued to anyone outside the agency's employment.

LIST OF PKI ELEMENTS TESTED

Certification issuance

Certificate revocation

Certification repository

Authentication

Non-repudiation support

Key backup

Key recovery

Client software

Integrity

NETWORKING REQUIREMENTS

An additional directory was added to the network with the intent of supporting a test of cross certification. This was not tested in the pilot. Without the requirement for testing cross certification, this directory would not have been added. Instead, the information stored in the directory would have been stored in the Novell directory.

TRAINING REQUIREMENTS

Support staff for digital signatures and electronic forms received no direct training. The digital signature infrastructure was established by Entrust and initially installed by them. During the installation, staff observed and was provided instruction on the operation and maintenance of the system. The electronic forms were developed without any formal training from developers studying the documentation. End-users required minimal amounts of training on the use of the electronic form or digital signature. Each employee was provided about 30-45 minutes of instruction specifically on e-forms and digital signature use. Specific training was provided for users of the electronic form and purchasing processes.

TESTING REQUIREMENTS

Attach a list showing all elements that were tested. This should include testing and validation of all elements of the pilot. Examples are registration and certificate issuance, infrastructure testing with the CA, server and network, simulation run through the entire system, bridge testing, application interface, connectivity functions (encryption and decryption), and use of test data to validate data exchange.

OBSTACLES

Technical issues: Experience a great amount of difficulty in the printing of some electronic forms. The requirement to print forms and the inability of the forms package to consistent print under certain conditions limited the form design and volume of content that could be collected. This also resulted in delayed implementation of some forms.

Early attempts with the electronic form were to use the form as a data entry screen for an application. The forms do not support sufficient connectivity and data testing logic to do this without a large amount of coding. It was determined that the forms greatest utility was for transmitting data and insuring that the data transmitted was what had been sent by utilizing the digital signature to secure the information. The form also provides a convenient method for routing information in a highly distributed environment such as DGIF for review and approval processes. The form also provides a secure mechanism for storage of the information with the digital signatures assuring integrity of the data for audit purposes.

The digital signature has proven to be very easy for employees to use. The cultural change of not having paper to handle has been the largest stumbling block.

Policy/legal: Many of the forms used by the agency that require a signature must go to an entity outside the agency. These forms still require wet signatures unless an agreement is reached with the outside entity to accept a digitally signed form. There is not a good way to securely indicate on a printed version of the form that it was in fact validly signed with a digital signature. Acceptance of the form is more on a trust basis because the “signature” could very easily be faked.

Business operations: The e-form has been directly associated with business process changes. The changes were not immediately embraced by all those involved. However, as some experience has been gained, employees have come to praise the electronic form and digital signature as a time saving and positive benefit.

The electronic form and digital signature are central to the agency’s plans for improving its administrative procedures. The technology is being integrated into all financial processes and in nearly all report filing processes used in the agency.

DEPARTMENT OF MOTOR VEHICLES (TAX AND TICKETS)

By David Bunn, Network Manager

PILOT DESIGN

We selected pilot projects that would be a viable test of the use of PKI from an Agency to locality (government to government). The pilots were not intended to be a designed solution to a business problem, but to replicate an existing process into an electronic environment.

With two of the pilots (‘Rental Tax’ and ‘Mobile Home Sales Tax’), we replaced a manual document that is produced at DMV from our records. The document is sent to the locality for certification, they may notate some revisions, and the document is returned to DMV for processing. In these pilots, we used PKI to sign/encrypt the data, and E-Mail to transport it as an attachment.

The additional pilot (‘Parking Ticket’ replaced the process where we send confidential data to a jurisdiction, with the transmittal of this data using E-Mail. The E-Mail attachment is used by the jurisdiction as an input data stream for automated processing at the recipients end.

The pilot PKI structure was provided by Entrust through VIPNet. The registration process was handled as follows:

1. The locality provided the DMV project manager with the name and E-Mail address of their pilot participants.
2. DMV provided the information to VIPNet to establish users on the CA
3. VIPNet sent an E-Mail to the end user with a ‘reference number’
4. VIPNet sent an E-Mail to the project manager with an ‘authorization code’ for each user
5. The DMV project manager contacted the end-user by phone and provided the ‘authorization code’.
6. The user was given instructions on how to obtain and install the Entrust PKI client. At installation, both the ‘reference number’ and the ‘authorization code’ were required to activate the client.

PRE-PRODUCTION

The pilot projects were implemented with the following sequence:

1. Install and activate client software. This included any networking changes required to communicate with Entrust.
2. Test the transmittal of signed and encrypted files, and the receipt of them on the other end. This was to insure that data flow was functional and trusted.
3. Transmit sample copies of data, and develop agreed upon data handling procedures.
4. Exercise a production level exchange of data following the agreed upon format.
5. Migrate the handling activity to the user level that would normally handle the data and develop the procedures that they need at their desktop.
6. Exercise the production run through the expected user levels that would handle production data.

In the course of implementation, we found countless difficulties with the exchange data being in the E-Mail body, and modified our process to have the data as an E-Mail attachment. Not only did that free us from formatting issues that SMTP apps imposed, but it removed any dependency on having a PKI-enabled E-Mail application.

BENEFITS OR SAVINGS EXPERIENCED

Met expectations, improved response time to Charlottesville and provided a development alternative for paper based reporting systems.

STAFFING

One Project Manager, associated support staff for technical development. Two users had PKI-Client software installed on their desktop and have exercised some PKI transaction functions.

FUNCTIONAL CONTEXT

We used digital signatures to sign packages of data. Some of the data packets were Reports formatted in Word. Some were mainframe generated, fixed-length data records. As this data was E-Mailed as an exchange between DMV and localities, we used encryption to secure it.

CERTIFICATE AUTHORITY

Entrust

LIST OF CERTIFICATES

6 certificates have been assigned and in use. 4 are for the project team to exercise. 2 are for end-user transactional activity.

LIST OF PKI ELEMENTS TESTED

Certification issuance

Certificate revocation

Certification repository

Authentication

Confidentiality

Key recovery

Client software

Integrity

TRAINING REQUIREMENTS

Janet Boyd (FAA) trained on how to send/receive PKI material. Initial training for 1 hr. 2 additional half-hour sessions were required. Training provided by D.Bunn.

Norma Southworth (SSG) was trained on sending PKI material. 1Hr. Training provided by D. Bunn

This training covered how to use the Entrust client. Procedures were developed for the users that outlined the steps for managing the data on the desktop, which included the use of PKI. The training walked the users through the procedure.

Additional involvement was required to keep in contact with the Fairfax, Charlottesville and Chesterfield localities and complete the cycle of testing. We worked through the process to be used at each of the localities and DMV developed and provided desktop procedures for the end-users at Fairfax and Chesterfield.

FAIRFAX COUNTY

By Jim MaGill, Information Protection Manager

PILOT DESIGN

At the end of calendar year 1999 initial discussions were conducted between representatives of DMV (state level) and Fairfax County. A subsequent meeting was held in Fairfax County where representatives of DMV met with representatives of Department of Information Technology (DIT), and Department of Tax Administration (DTA), Fairfax County. At this meeting the DMV pilot was explained and discussions ensued relative to Fairfax County' participation in this pilot. Fairfax County agreed to participate. This decision was based upon Fairfax County's desire to expand its E-Government activities and the amount of effort that would be necessary to support participation in this project. The pilot was determined to be low risk and require only minimum resources.

As the DMV project was explained, activities currently accomplished using hard copy reports would be conducted using electronic means without the need for sending and receiving hard-copy reports between DMV and Fairfax County. The two reports being considered for this pilot were revenue-related reports. One report dealt with the sales tax received on rental vehicles and the second report dealt with revenues from mobile home sales. Hard copy reports were received from DMV on a quarterly basis, received in the DTA office, reviewed and reconciled and then a marked-up hard copy of the report was mailed back to DMV. With this pilot, reports would be generated at DMV and transmitted electronically to Fairfax County and when Fairfax County completed the verification and reconciliation, a digital signature would be affixed to the electronic copy that would then be transmitted back to DMV.

Initial discussions relative to the design of the project concluded that e-mail would be used to transmit the report. Since e-mail systems in use were different it was decided that the report would be transmitted as part of an e-mail rather than as an attachment. Upon receipt of the electronic report within the DTA, Fairfax County processing would be accomplished using the current process in place with virtually no change in the duties of the individuals involved in the manual process. The Information Protection Branch (IPB), DIT, Fairfax County, would act as to focal point for the pilot and would control the issuance, use and management of the supporting certificates and keys that would be used to support this activity.

Fairfax County's activities were in support of the DMV pilot and were not, at this time, considered to be a separate pilot. Since we (Fairfax County) were participating in a pilot that was primarily already designed by DMV our design efforts centered on designing implementation activity that provided support to the overall design of the pilot by DMV.

PRE-PRODUCTION

Prior to going into production, preparation work was required to ensure that the infrastructure would be in place to support pilot activities. Initially the current process in use within DTA needed to be identified and analyzed to determine what was being accomplished, how the actions were being accomplished, and also identify the levels of responsibilities. Once the process was understood a strategy had to be developed to introduce the use of digital signatures. Another area that needed to be explored was that of determining the efforts needed to obtain, implement and continue support digital signature activities once they were implemented. In addition, an oversight and monitoring role had to be determined.

Internal Fairfax County meetings were held between Fairfax County DIT representatives and Fairfax County DTA representatives. During these meetings the process in effect (a manual process of receiving a hard-copy report, processing it, and returning the corrected and verified copy to DMV) was analyzed. Individuals, roles, and duties were identified; levels of control and supervision were also identified, and verification procedures were also identified. The electronic system components and activities were discussed and a strategy developed as to how this infrastructure would be introduced into the existing process.

The electronic process was designed to retain the roles, duties, and oversight currently in effect. Individuals were identified who would receive the report, review it and make the changes. Report review levels were identified and the individuals who accomplished these actions were identified. The final approval authority was identified along with the individual who performed this function. Once this process flow was fully identified, the points where the digital signature would be affixed and by whom was determined. Then the number of certificates needed along with to whom they would be issued was determined.

Additional discussions were held with DMV to further define specifics as to how changes on the report would be recorded. Options were discussed and eventually DTA representatives and DMV worked together to decide report format, how changes would be recorded, and report submission details.

Concurrently, representatives of the Information Protection Branch, DIT, identified the basic measures necessary to receive, issue, and maintain digital certificates necessary to support this program. One member of IPB was assigned this role and developed a process to obtain, issue and maintain certificates. He also worked with DSI members to obtain further specifics concerning characteristics of the certificates, details relative to receipt, storage and maintenance, and how these certificates would be transmitted to Fairfax County. As more details became know modifications and expansion of the basic measures were made. The IPB representative then developed a strategy to obtain, issue, and manage certificates and to also monitor subsequent related activities.

IPB representative worked closely with VIP-Net/Entrust to obtain specific details necessary for obtaining, issuing, and maintaining certificates. The first certificate was received by IPB representative, who installed the certificate on his platform and performed testing with VIP-Net/Entrust to ensure that it was fully functional. Once this was done, testing continued with representatives of DMV to ensure that an e-mail could be sent and received, and encrypted and decrypted using this certificate. Once this was successfully accomplished, additional certificates were obtained and issued by IPB to members of DTA.

A supervisor within the DTA identified individuals who required certificates. Individual identify was verified by the IPB representative prior to issuance of the certificate. Identity was confirmed by using a combination of factors. All employees are entered into the personnel database within the County, each individual has a unique UserID, and every employee must have a picture identification badge. Once identity was confirmed the certificate was issued.

The IPB representative did individual one-on-one training with DTA employees. Test messages were then sent and received between DMV and DTA and were successful. Messages could be sent and received and could be encrypted and decrypted successfully. The system was now in full production for the pilot and was monitored by IPB representatives.

PLANNED PROJECT COSTS

None other than normal daily operational costs

ACTUAL PROJECT COSTS

No significant additional costs – all were included in normal daily operational expenditures.

EXPECTED BENEFITS

Better understanding of the necessary components to employ a practical application of digital signature; better estimation of costs associated with employment of digital signature and PKI within Fairfax County; and better understanding of the infrastructure needed to support digital signature and PKI.

BENEFITS OR SAVINGS EXPERIENCED

Most expectations were met but some were not met in the detail desired due to lack of specific details unknown to the project. As more time passes, more details will result.

STAFFING

CIO, Fairfax County

Staff: 2 members from the Information Protection Branch (1 was the Pilot Project Lead and one was the back-up and administrator for installation and maintenance for certificates; four staff members from the Department of Taxation (2 representatives for each pilot activity (i.e. 2 for Rental Sales Tax and 2 for Mobile Home Tax)).

FUNCTIONAL CONTEXT

Describe the functional context in which you tested digital signatures. How were you trying to use them? Digital Signatures were used in place of “wet” signatures. E-mail was sent from DMV to the County. This e-mail contained a taxation report. This e-mail was routed to the appropriate section within Fairfax County Department of Tax Administration (DTA). The report was reviewed and any changes made in e-format. Once ready for transmission back to DMV, the report was digitally signed and e-mailed back to DMV.

APPLICATION ENVIRONMENT

List the existing hardware, software, telecommunications or other services that were in place, and list new elements in all categories needed to enable digital signatures.

Users were on desktop platforms using Windows 95 or 98. Telecommunication used existing channels from DMV and Fairfax County; Entrust certificates were used; Outlook E-mail was used from the County to the State. New elements needed were the Entrust certificates and services to support installation and maintenance of the certificates.

CERTIFICATE AUTHORITY

Entrust

LIST OF CERTIFICATES

Five Certificates were used. One in Information Protection Branch for oversight and general on-site support; 4 in Department of Tax Administration.

LIST OF PKI ELEMENTS TESTED

Certification issuance

Authentication

Confidentiality

Key recovery

Integrity

NETWORKING REQUIREMENTS

Software (Certificates) was installed at the desktop level.

TRAINING REQUIREMENTS

Project Lead was initially trained on procedures to be followed; 1 person in the Information Protection Branch was trained on technical aspects of obtaining, installing, and maintaining certificates. This individual trained all others.

TESTING REQUIREMENTS

Messages containing test data and subsequent messages containing actual report data were sent and received to test:

- Certificate Issuance
- Connectivity with Certificate Authority and with DMV
- Correct functioning of certificates
- Encryption
- Network Connectivity with DMV

CHESTERFIELD COUNTY

By Sandy Graham, Data Security Administrator

PILOT DESIGN

Chesterfield County selected a digital signature pilot process that would allow functionality testing of basic PKI concepts during exchange of business information between a state agency and a Chesterfield County department. Chesterfield County entered into partnership with DMV on the selection of the Reimbursement Approval for Mobile Home Sales Tax and Additional Rental Sales Tax as pilot applications.

Chesterfield County selected its vendors for the pilot project to be comparable with their pilot partner, DMV. GroupWise 5.5.2 was chosen as our email client because it was already Entrust/PKI enabled and was a part of our installed technical infrastructure environment. Our network operating system of Novell 5.0 would support the pilot project without any required upgrades. Entrust PKI 5.0 was selected as the PKI desktop solution to be compatible with the DMV desktop solution.

The pilot project affected a small group of customers closest to the business process, all within the Chesterfield County Commissioner of Revenue department. Originally it was thought that the Treasurer's Office would be involved in the project to facilitate deposit of the tax reimbursement. It was decided that the scope of the pilot project would only include electronic approval of the reimbursement and the deposit (done through EFT) would not be included in the workflow of the pilot. The pilot project involved transactions produced quarterly, so the volume of test data was small and would only address one formal quarterly business cycle for the reporting period of May 2000 through July 2000. These business applications prior to the pilot produced quarterly hardcopy financial reports, which required transport via U.S. Postal Service between Chesterfield County and DMV. The scope of the DSI/PKI project was to automate this time-consuming process by utilizing secure electronic mail as the transport vehicle.

The pilot project utilized Digital signatures within an electronic mail format only and did not include any application integration. The signature was not programmed into an application nor was any programming logic associated with the signature itself to trigger other transactions. The pilot project scenario is described as:

1. A financial report was sent to Chesterfield County from DMV for approval of Tax reimbursements.
2. The financial report was sent by DMV in an encrypted format to ensure citizen privacy of address information and digitally signed by DMV to ensure authenticity.
3. Upon receipt, Chesterfield County evaluated the financial report received as a Word attachment. Chesterfield County Commissioner of Revenue staff evaluated and corrected the content of the financial report with notations as appropriate.
4. Appropriate Chesterfield County Commissioner of Revenue staff thereby denoting approval digitally signed the document.
5. The financial report email and attachment was encrypted for privacy.
6. The approved financial report e-mail was electronically sent back to the DMV point of contact.
7. Following receipt of the approved financial report, DMV staff investigated corrections.
8. If corrections were required, DMV staff made adjustment entries. If the financial report is approved as is, the reimbursement request was initiated by DMV.

Chesterfield County involved the end-user, Data Security Administration, Technical Services, Network Services, and Information Center in gathering design requirements for the PKI environment. The PKI pilot project roles were defined as follows:

- End-User: Utilize desktop client software to test the business process
- Data Security Administrator: Coordinate request, approval, assignment and revocation of Certificates
- Technical Services: Evaluate and recommend communications protocol solutions (i.e.,
- TCP/IP issues, etc.)
- Network Services: Evaluate and recommend network access solutions (i.e., Port and/or firewall issues, etc.)
- Information Center: Install desktop client components

PRE-PRODUCTION

The production environment included utilization of VIPNET as the Certification, Registration, and Revocation Authority. Chesterfield County was required to open ports within our firewall to allow communication with the VIPNET bridge. GroupWise 5.5.2 was the email client utilized to transport the electronic records.

Entrust PKI 5.0 was installed as a demo product on five client workstations participating in the pilot. Each participant was issued a digital certificate. This process required the requestor to make the request for the certificate in-person or face-to-face to the Data Security Administrator. Upon validation of the request, the Data Security Administrator submitted a request in writing via electronic mail to the VIPNET Registration Authority contact. The VIPNET Registration Authority contact then added the username and password of the certificate requestor. Notice was given to the VIPNET Certificate Authority to issue a certificate to the requestor. The VIPNET Certificate Authority then issued the Entrust Certificate and Reference Number to the requestor via electronic mail. At this time the requestor could activate the Entrust client software and utilize the digital certificate.

The Pilot was separated into two Phases. Phase One was used to evaluate the PKI client software, hardware and network components required to allow customers in the Commissioner of Revenue department to exchange secure electronic documents, encrypted and/or digitally signed, over the existing countywide network. The electronic documents were exchanged as e-mail attachments. The tasks associated with implementation of the pilot project included:

- Identification and implementation of workstation software, network and server infrastructure requirements
- Novell 5.0 NOS
- GroupWise 5.5.2
- Entrust PKI 5.0
- VIPNET as CA/RA

Chesterfield County, DMV, and Entrust participated in a technical conference call to review the technical requirements for participating in the pilot. It was important the two partners (Chesterfield and DMV) have comparable email clients that were PKI enabled by Entrust. Possible options included Microsoft Outlook Express or GroupWise 5.5.2. Chesterfield County selected GroupWise 5.5.2 due to it already being installed. At least version 5.0 of the Novell NOS was required, which Chesterfield County had installed already. Once the decision on software products were agreed upon, Chesterfield County just needed to wait on Entrust to deliver the PKI 5.0 client and for VIPNET to issue the certificates.

- Testing proof-of-concept of secure electronic mail and the use of digital signatures within county departments (Information Systems Technology)

  IST staff tested proof-of-concept by exchanging email documents between themselves and with DMV project staff.

- Identification and resolution of issues that may affect production implementation and deployment of PKI-enabled business processes with DMV

  Process flow issues were encountered regarding making adjustments or corrections prior to approval of the financial report. A method was identified wherein a change summary would be documented within the email attachment as approved adjustments.

Phase II included the utilization of the PKI infrastructure to communicate with a state agency (DMV) in support of testing electronic exchange and digital approval of the Mobile Home Sales Tax and Additional Rental Sales Tax reports. The tasks associated with Phase II included:

- Verification of the successful exchange of data between DMV and Chesterfield County

  Data was exchanged between DMV staff and Chesterfield County Commissioner of Revenue staff. Few adjustments to the process were recommended to ensure that persons that normally would route the document for validation prior to approval would still be involved in the electronic process.

- Identification and resolution of issues affecting the timely implementation and deployment of PKI for the pilot process

  No major issues arose in the final exchange of data between Chesterfield County and DMV.

The project involved approximately 5 users from the Commissioner of Revenue department, the Treasurer's Office and Information Systems Technology. Other resources utilized for the pilot project includes;

1. Software licenses, training and support for client PKI components (at no cost),
2. VIPNET as the Certificate Authority for the Pilot (at no cost),
3. Project Leader from DMV
4. Project Leader from Information Systems Technology
5. Application Development Staff
6. Two users from each participating department

The pilot utilized Chesterfield County's existing workstation and network infrastructure. No new hardware, system or software upgrades were required. The client desktop software was provided as a demo by Entrust at no cost. Limited training was provided in-house by staff that attended the PKI Education Day held at UVA. Costs for participating in the pilot were negligible, although we recognize that future PKI production deployments would require training, software, and staff support costs.

PLANNED PROJECT COSTS

None. Project expectations were that the vendor would supply a demo product at no cost to the pilot participants.

ACTUAL PROJECT COSTS

None. Entrust vendor provided client software as a demo product at no cost to pilot participants

EXPECTED BENEFITS

Knowledge of PKI infrastructure requirements and practical lessons learned in the use of PKI in a live environment. Better understanding of e-government implications to business processes and potential changes and/or improvements to delivering customer services.

BENEFITS OR SAVINGS EXPERIENCED

The PKI pilot was a rewarding experience for Chesterfield County in that we got to experience first-hand the technical requirements for support of an infrastructure framework for PKI, the business process changes/improvements required, and the time savings on exchange of electronic approvals versus hardcopy approval exchange through U.S. mail. On average, the approval process for Mobile Home Sales Tax took up to one full month using the old process. With electronic signature approval, the process now takes less than seven days from point of receipt to final approval and report transmission.

STAFFING

Existing staff was utilized for the PKI project. A project leader and co-project leader was assigned to ensure the technical aspects of the project were completed on-task. Four end-users actually responsible for utilizing the electronic process for an existing approval process were involved in the project to execute and analyze the test data.

FUNCTIONAL CONTEXT

Chesterfield County only utilized Digital signatures within an electronic mail format. The signatures were not programmed into an application nor that any programming logic associated with the signature itself to trigger other transactions. The pilot scenario is described as 1) a financial report being sent to Chesterfield County from DMV for approval of reimbursements. 2) The document was sent in an encrypted format to ensure citizen privacy of address information and digitally signed by DMV to ensure authenticity. 3) Upon receipt, Chesterfield County evaluates the financial report received in a Word attachment format, evaluated and corrected content with notations as appropriate. 4) The document is then digitally signed thereby denoting approval. 5) The email and attachment is encrypted for privacy. 6) The e-mail is electronically sent back to the DMV point of contact. 7) Following receipt of the approved financial report, DMV staff investigates corrections. 8) If corrections are required, adjustment entries are made. If the financial report is approved as is, the reimbursement request is initiated by DMV.

CERTIFICATE AUTHORITY

VIPNet

LIST OF CERTIFICATES

Five certificates were issued.

LIST OF PKI ELEMENTS TESTED

Confidentiality

Privilege/policy creation

Client software

Privilege/policy verification

TRAINING REQUIREMENTS

The pilot team leader, associate and additional network staff attended the full day Digital Signature Education Day held at UVA. This 1 day of training was sufficient for the pilot participation however, to support a PKI project within Chesterfield County, would require PKI administration training by information security staff and technical training for those responsible for installation and maintenance of the PKI technical infrastructure. The end-users of PKI would require awareness training of security, privacy and authentication issues, and the responsibilities associated with utilizing e-government exchange of transactions using PKI.

WISE COUNTY

By Arnold Thielen, President, MIXNET Corporation

PILOT DESIGN

The Circuit Court for Wise County/City of Norton, VA (hereinafter referred to as: “the Court”) processes a large number of legal documents on a daily basis. These hardcopy documents are filed by various organizations (e.g. Local, State, Federal Government Agencies, lawyers, courts) and the general public through a visit to the Circuit Court Office. Once the documents are filed and stored with the Circuit Court Office they are in demand by various organizations.

The goal of the pilot is to enable the filing, searching and retrieval of public Circuit Court documents remotely and electronically.

The Court has approximately 120 different types of documents. Portions of these documents appear on all documents and other sections are distinct from document to document. Throughout the pilot we selected one instrument type or document (DEED OF TRUST) to be filled electronically by the local Housing Authority.

Throughout the pilot we examined various types of software that would enable a secure, fast and affordable electronic filling. We evaluated products by ADOBE, PUREDGE, JETFORM, MICROSOFT, XMLS and others. In order to keep the cost for the participants down and to ease the installation and support, we decided to develop and implement a workflow application in HTML.

The design process was completed by MIXNET CORP.

PRE-PRODUCTION

1. Analysis of the user document flow requirements;
2. Analysis of the Court document administration requirements’
3. Analysis of the legal requirements of the document (signature, original versus copy, authors rights to change the document, other participants rights to change the document, finalization of document)
4. Identification of different electronic signature alternatives:
    - Digitized hand signed signature through a signing pad;
    - Digitized hand signature with biometric verification;
    - Digitized signature in combination with a digital signature;
    - Digital signature only.

We reviewed these different signature options with the participants.

1. Identification of procedures on how to control the document creation process since multiple parties are involved in the document creation, review and administration of the document;
2. During system design we included system requirements that are applicable beyond the pilot. Based on those finding we developed the pilot.
3. Time of implementation: Research, Testing, Development, Configuration, Installation, Training: 320 hours
4. Pilot Budget: $ 18,000

The efiling application will be integrated with the electronic search and retrieval application. The level of security of the application also impacted the level and type of electronic signature.

PROJECT SCOPE & OBJECTIVES

The pilot project is a secure web based electronic filing (hereinafter referred to as “efiling”) application of Circuit Court instrument documents between the filing agency Big Stone Gap Housing Authority (HUD affiliate), a law office, a notary public and the Wise County/City of Norton Circuit Court office. The design and implementation procedures of the efiling process are provided by MIXNET CORP.

SHORT TERM PILOT PROJECT GOALS:

The goal of the pilot project is to prove technically and economically that document filing, searching and retrieval of Circuit Court instruments can be accomplished between Government agencies and the Circuit Court Office through electronic filing in a faster, safer, cheaper and more secure way for all participants then the existing methods in place.

LONG TERM PROJECT GOALS:

The long-term goal of the project is to expand efiling to non-government agencies (i.e. law offices) and to implement the final efiling pilot project model as a working production efiling concept for all Circuit Courts in the Commonwealth of Virginia and other government agencies. The pilot will only be successful in the long run if the following goals are achieved:

1. Increase the speed and accuracy of document filings;
2. Reduce the time and cost of document filings and document management;
3. Reduce the technology investment within Circuit Court Offices;
4. Reduce the local IT “burden” of Circuit Court Office;
5. Make the documents and instruments available to the public up to the minute (24 hours/7days);
6. Build a platform that is safe and secure and that always incorporates the latest proven technologies;
7. Suggest and help create standards for the Dept. of Information Technology Land Records Management Task Force that can be implemented for 121 Circuit Courts within the Commonwealth of Virginia.

PLANNED PROJECT COSTS

(BEYOND PILOT)

1.	Efile/workflow application development:	$13,000
2.	Secure and legal signature software:	$1,500
3.	Hardware	$5,000
4.	Installation, Testing, Training, Support:	$ 14,000
	Total:	$ 33,500

ACTUAL PROJECT COSTS

The cost listed under 6. is beyond the cost of the pilot and is based on the implementation of an efiling application for all Circuit Court documents.

The total cost will increase as participants in efiling will increase, however the cost per user will decrease.

EXPECTED BENEFITS

File documents with Circuit Courts faster, safer, cheaper and more secure 24 hours/7days. Decrease the document management cost for Circuit Court offices and increase the availability of Circuit Court public records to the public to 24 hours/7 days.

BENEFITS OR SAVINGS EXPERIENCED

We met the first set of short-term goals of pilot project. The long-term goals are not yet achieved and it was not planned to have them achieved during the pilot.

STAFFING

3 staff members were involved.

PROJECT PLAN

www.efile.com

CERTIFICATE AUTHORITY

Department of Information Technology / VeriSign

LIST OF CERTIFICATES

Four certificates were issued.

LIST OF PKI ELEMENTS

Certification issuance

Authentication

Privilege/policy creation

Key backup

Secure time stamping

Integrity

Notarization

NETWORKING REQUIREMENTS

No additional changes necessary for the pilot; changes will be needed for a broader implementation.

TRAINING REQUIREMENTS

All pilot participants of the efiling of Circuit Court documents have been trained.

ACQUISITION AND INSTALLATION ACTIVITIES

Raid 5 level hardware installed and tested;

Server and client based signature software purchased and installed;

Parallel server software planned to install for future use;

Workflow software planned to install for future use.

OBSTACLES

Technical obstacles: Currently in process of installing an electronic biometric signature combined with digital signature for web based html application;

Policy/legal obstacles: Identification which level of electronic signature will meet FUTURE legal requirements. The identification on what is a legal signature in a given application environment will be an issue for the future.

The policy/legal issues are the greatest uncertainties for our pilot.

No business operations obstacles.

DEPARTMENT OF INFORMATION TECHNOLOGY

By Jim Adams, Sr. Information Technology Manager; Wayne Robertson, Director of Management Information Systems; and Sally Fehn, Security Division Consultant

PILOT DESIGN

APPLICATION SELECTION

DIT reviewed applications owned by DIT for a potential candidate to be a part of the Digital Signature Pilot Project. The criterion for selection of an application included such items as: was a signature required from the customer, who were the customers, was it a legacy application, and would there be a cost saving, either tangible or intangible?

DIT selected a telecommunications application that, if placed in production status, could be used to interact with 2500 telecommunication customers across the state. That application is driven by a legacy system using a The Telecommunication Service Request form (TSR), which could be submitted one of several ways, and the question was, could the process be web enabled? The answer was yes. Several vendors provide Web enable solutions to the mainframe through middle-ware software or Application Program Interfaces (API). Discussions were held with these software vendors and System Integrator’s to determine previous experience with this process. The same process was done with electronic forms vendors. Vendors who participated were Software AG, SAGA SOFTWARE, SHANA FORMS, and PureEdge. The vendors selected were SAGA SOFTWARE and PureEdge because they had worked together in the state of Texas and Alaska. DIT made a decision to partner with VeriSign for the digital certificate for our pilot users.

ISSUE CERTIFICATES

The Department of Information Technology (DIT) is acting as a Local Registration Authority (LRA) under the VeriSign Class 2 Primary Certificate Authority (CA) for purposes of the pilot. To issue certificates under this CA root certificate, VeriSign delegated the responsibility for identification and authentication of certificate subjects to DIT. Procedures were developed and distributed to the Digital Signature Initiative workgroup to define the process of obtaining a digital certificate during the pilot. DIT does not sign or issue certificates, but controls the passcodes to receive a certificate from the VeriSign CA. Once a certificate subscriber has been uniquely identified, the LRA uses an administrative certificate to create a passcode through a VeriSign website. The passcode is available during a window of time to the subscriber to download their digital certificate signed by the VeriSign root CA. The following paragraphs are from the LRA procedures document and explain the three processes available to register to receive a digital certificate during the pilot.

APPENDIX G

ROLE OF THE LOCAL REGISTRATION AUTHORITY

The Local Registration Authority (LRA) will insure that the certificate subscriber has provided documentation that demonstrates unique individual identity. There are three approaches for verifying the identity of the subscriber:

1. Face-to-face registration before the LRA
2. Videoconference registration before the LRA
3. Notary Public registration and mailing to the LRA

In addition, for the digital signature pilot, the subscriber must be on the list of Telco Coordinators that was provided by the manager of Telecommunications Customer Support or on the list of named Wise County clerks. Only the designated individuals will be provided, through a person-to-person method, a passcode to gain access to the Digital Signature Website links to begin registration for the pilot project.

The process begins by the subscriber choosing and proceeding with one of the three approaches listed above to obtain their digital certificate.

After establishing the proper identification of the subscriber through one of the identification processes, the LRA provides the authentication passcode to the subscriber. The subscriber will proceed to access the VeriSign website to download their individual digital certificate. Once the certificate and private key have been downloaded to the user's machine it is a good idea to create a password-protected copy on a diskette. Instructions are on the www.dit.state.va.us digital signature pilot website.

ACCEPTABLE IDENTIFICATION

To demonstrate a unique individual identity, the subscriber must provide two pieces of identity, one from list A and another from either list A or list B.

LIST A:

A photographic ID issued by a State or Federal government

A valid state Drivers License or

A Passport or

A Military Identification Card or

A State/Federal Identification Card

LIST B:

A Social Security Card or

A credit card or

A Certified Birth Certificate

The LRA records the piece of identity from list A that was presented, including it's ID number, as part of the certificate registration process, but does not record the number from the piece of identity from list B, only uses it to verify the individual identity. The LRA maintains its registration records as confidential documents.

FACE-TO-FACE REGISTRATION

1. The subscriber downloads, prints, and completes Section A of the DIT Certificate Registration form (.pdf, 295 KB)., available through the DIT homepage at http://www.dit.state.va.us/security/digsig/pilot/ , and then e-mails the DIT LRA, Sally Fehn, Sfehn@dit.state.va.us to arrange for a face-to-face registration for a digital certificate.
2. To demonstrate a unique individual identity, the subscriber must present two pieces of identity, one from list A and another from either list A or list B.
3. The LRA verifies validity of the subscriber request by checking the list of pilot participants and either proceeds with the process or denies certification based upon an invalid identity.

4. The LRA lists the forms of identification presented and attests to the identity of the subscriber by signing the certification form.
5. The LRA provides the subscriber with information about the importance of keeping the private key and certificate secure found on the VeriSign web site at: https://onsite.verisign.com/services/VADeptofInformationTechnology/client/help/concepts/didprotect.htm. The subscriber signs the form to acknowledge their understanding of the subscriber responsibility to protect the key and certificate.
6. The LRA provides the subscriber with the passcode to enter when enrolling for the certificate. The subscriber signs the form to indicate they have received their passcode.
7. The subscriber proceeds to follow instructions on the DIT website http://www.dit.state.va.us/security/digsig/pilot/ under 4. Download your digital certificate.

Videoconference Registration

1. The subscriber downloads, prints, and completes Section A of the DIT Certificate Registration form (.pdf, 295 KB)., available through the DIT homepage at http://www.dit.state.va.us/security/digsig/pilot/ , faxes it to 804/371-5505, and then e-mails the DIT LRA, Sally Fehn, Sfehn@dit.state.va.us to request a videoconference..
2. The subscriber appears before the LRA to verify their identity via a prearranged videoconference.
3. To demonstrate a unique individual identity, the subscriber must present two pieces of identity in front of the camera, one from list A and another from either list A or list B.
4. The LRA verifies the validity of the subscriber request by checking the list of pilot participants and either proceeds with the process or denies certification based upon an invalid identity.
5. The LRA lists the forms of identification presented and attests to the identity of the subscriber by signing the certification form.
6. The LRA provides the subscriber with information about the importance of keeping the private key and certificate secure found on the VeriSign website at: https://onsite.verisign.com/services/VADeptofInformationTechnology/client/help/concepts/didprotect.htm. The subscriber signs the form to acknowledge their understanding of the subscriber responsibility to protect the key and certificate.
7. The LRA provides the subscriber with the passcode to enter when enrolling for the certificate. The subscriber signs the form to indicate they have received their passcode.
8. The subscriber proceeds to follow instructions on the DIT website http://www.dit.state.va.us/security/digsig/pilot/ under 4. Download your digital certificate.

Identification by a Notary Public

The registration process is assisted using a Notary Public in the role of the LRA in the event that face-to-face or videoconferencing is not available.

1. The subscriber downloads, prints, and completes Sections A and B of the DIT Certificate Registration form (.pdf, 295 KB)., available through the DIT homepage at http://www.dit.state.va.us/security/digsig/pilot/.
2. The subscriber reviews information about the importance of keeping the private key and certificate secure found on the VeriSign website at: https://onsite.verisign.com/services/VADeptofInformationTechnology/client/help/concepts/didprotect.htm. The subscriber signs the form to acknowledge their understanding of the subscriber responsibility to protect the key and certificate.
3. The subscriber takes the application to be notarized. The Certificate Registration form contains fields for the elements in the certificate: name, E-mail address, agency ID (4 numeric positions), and phone number.
4. The Notary Public attests to the identity of the person listed in the certificate application and verifies the true identity of the individual. The notary then notarizes the Certificate Registration form attesting that the applicant's identity has been verified.

   The notarized Certificate Registration form serves as a legal document verifying the identity of the person listed in it, and protects the entire process under existing law in all 50 states. Under existing law, it is illegal to show a false identity to a Notary Public.

5. The subscriber mails the notarized Certificate Registration form to the LRA.
6. The LRA verifies the validity of the subscriber request by checking the list of pilot participants and either proceeds with the process or denies certification based upon an invalid identity or lack of notary seal and signature.
7. The LRA returns a sealed envelope through certified mail to the subscriber containing a second sealed envelope with the passcode and next step to download the individual digital certificate, and a document to return to the LRA acknowledging the receipt of the passcode.
8. The subscriber returns the signed document verifying that they received the passcode.
9. The subscriber proceeds to follow instructions on the DIT web site http://www.dit.state.va.us/security/digsig/pilot/ under 4. Download your digital certificate.

ASSURANCE LEVELS

Only certificates following a high assurance policy were issued during the pilot. Two pieces of identification, one with photograph, must be presented in person before the LRA or a Notary Public to uniquely identify the certificate subject.

POLICIES

The VeriSign Certificate Practice Statement (CPS) was modified for internal purposes of the pilot to reflect distributing certificates under only one policy for Class 3 certificates, high assurance level.

PARTICIPANTS

The DIT team included Jim Adams, Wayne Robertson, project manager, Sally Fehn, project coordinator; Gary Esslinger, application support; Kathy Belbin and Eric Schwartz, systems engineering; John Gordon, MIS staff forms design; Bob Baird and Ron Moore, Web support; and Stephanie Saccone and Susan Martin, Web page support.

IMPLEMENTATION STRATEGY

VeriSign issues policies covering the Certificate Practice Statement under the Public VeriSign offering. Procedures developed consisted of:

- Local Registration Authority
- Using the TSR Form
- Help Desk
- WEB procedures for How To Do ….

The application deployment was to setup a Web enabled front end to access and update a mainframe legacy database. Application Integration involved creating a Web enabled Electronic form, applying a digital signature, installing and configuring middle-ware and Application Program Interface (API's) to access a legacy application database residing on an IBM mainframe.

Procurements were needed for: SAGA SOFTWARE for consulting services to develop and install the middle-ware software and API's; PureEdge for the electronic forms and licenses for 21 users; and VeriSign for their Onsite Services and 50 certificates to be used to digitally sign the TSR form. Funding for the pilot was provided by DIT. The certificates and electronic forms licenses were provide at no charge to the users for the pilot demonstration.

RESOURCES

Resources for the project include: project dates from the middle of November to present.

- DIT recruited a P14 specifically for digital signatures. Working at least 25 hours a week for two and a half months this position has been functioning as RA, problem analysis and developed policies and procedures.

- DSI Work Group Lead.
- Project Manager.
- Application and Systems Programmers – two full weeks of application changes.
- Web development and deployment – 5 weeks of development.
- Additionally, partnering vendors provided extra resources and time to the pilot.

ACTUAL PROJECT COSTS

Time allocated by resources has exceeded any expectation of supporting the pilot.

BENEFITS OR SAVINGS EXPERIENCED

Problems that occurred during the pre-production period, the month of June and July, the application hasn't had the availability expected. Those problems are resolved and production availability should be obtainable during the month of August.

FUNCTIONAL CONTEXT

The digital signature provided the means to replace the current paper process requiring a signature with a Web-enabling Telecommunications Service Request form (TSR). The TSR form functions as the contract between the agencies and DIT, acting as an intermediary, to request service from the phone company. The agencies are subsequently billed for the service. The interactive form allowed the Telco Coordinators at the agencies and county offices to enter the TSR information and digitally sign it, submit it, and receive back an order number. Seventeen Telco Coordinators were authorized to receive a digital certificate and participate in the pilot by entering data into the interactive form that updates the mainframe production database.

CERTIFICATE AUTHORITY

VeriSign

LIST OF CERTIFICATES

Out of the thirty-two certificates that have been authorized, twenty have been requested and issued to-date. The other twelve coordinators have not requested to participate in the enrollment process so the certificates have not been distributed. Seven are for use by DIT staff to test and maintain the pilot. Three have been issued for use in a pilot by Wise County. The remaining ten certificates are in use by agencies and county offices to enter TSR forms.

DEPARTMENT OF MOTOR VEHICLES (TRAVEL REIMBURSEMENT)

By Gerald Rowe, Unisys Project Manager; Debbie Dodson, DMV Project Manager; and Lana Shelley, DMV Project Manager

PILOT DESIGN

The Unisys PKI Proof of Concept (PoC) was designed to educate the DMV user community on the benefits of digital signatures in an electronic, end-to-end PKI application that implemented emerging technologies such as XML, smartcards, biometrics, web access control, and electronic workflow. By selecting an existing signature-driven application, such as Travel Reimbursement, our PoC identifies and quantifies the factors contributing to a business case of replacing paper documents and manual workflow with a paperless, electronic solution that is determined and secured by digital signatures.

The selected solution allowed DMV an opportunity to document Unisys migration methodology for secure electronic workflows, discuss and document the legal, technical, and operational issues associated with a PKI-enabled applications, and assess the training and support needs of an electronic workflow application. The Unisys solution integrated various PKI vendors' offerings, such as Baltimore Technologies' Certification Authority, ValiCert's Validation Authority, Unisys Web access control and electronic workflow software packages, PureEdge's XML form designer/viewer, and various token vendors' products.

Unisys provided and installed the enabling software components for the PoC on each DMV participant's workstation. During the Unisys PKI PoC, DMV travelers and approvers were issued digital certificates that were used to sign travel requests and reimbursement documents. Participants attending the training sessions were provided with a step-by-step instructional guide, directing them to request and install personal certificates. Participants were then instructed to enroll into the web access control database. Upon receiving either a verbal or email confirmation to a successful enrollment, the participants could access the secured Travel Request and Reimbursement electronic forms with the proper credentials – digital certificate, pin, and unique ID.

Travelers were asked to enter their travel requests and travel expense information on electronic forms and scan their receipts and electronically attach them to the reimbursement form. Once the request for travel approval or reimbursement was submitted, the approvers were instructed to check their workflow inbox and act on each request, as they would in the manual process. After the forms were digitally signed by each approver, processed and archived, the auditor would verify the forms for accuracy and validity of the digital signature (i.e., ensure that the signature was not revoked or suspended during the signing process).

PRE-PRODUCTION

Our strategy for implementing the PoC was based on the Unisys four-step methodology of determining the Proof of Concept requirements, designing the application, delivering the solution, and detecting progress by monitoring the effectiveness of the PKI solution.

First, detail requirements were determined during a post Proof of Concept kick-off meeting. Unisys consultants documented the responsibilities, technical requirements, and expectations in a Requirements Specification Document that was delivered to the DMV project managers.

Next, Unisys consultants engineered a PKI-secured, electronic workflow for the DMV application. Electronic forms were designed and constructed to imitate the DMV travel request and reimbursement paper forms. In an effort to simplify the project for the participants, who would be required to fill out both electronic and paper forms during the duration of the PoC, we decided to use the electronic format for both the manual and electronic workflows.

For testing purposes, the DMV application was duplicated at the Unisys Center of Excellence. However, certain integration tests could only be performed during the onsite installation, such as unique network configurations and firewall policies.

The specific requirements of an on-site Registration Authority and a web-based workflow application were ideal for illustrating the benefits of web-access control, electronic workflow software, and the Unisys Certification Authority using Baltimore Technologies' PKI software. To complete the PKI design process, Unisys provided the Certification Practice Statement (CPS) for the DMV implementation of the CA's supported Certificate Policies (CPs).

Lastly, the Unisys staff provided the installation, training and management staff for a successful implementation of the PoC in the DMV environment. The bulk of the installation was accomplished within a five-day period. Training was provided in several sessions based on participants' availability and projects' complexity. In addition, several one-on-one training sessions were held to train the various DMV technical support staff. These sessions included training the Registration Authority, the Web Access Administrator, and the InfoImage (electronic workflow) operator.

PROJECT SCOPE & OBJECTIVES

The DMV Travel Authorization and Reimbursement Digital Signature Pilot was designed to educate the DMV user community on the benefits of digital signatures in an electronic, end-to-end PKI application that implemented emerging technologies such as XML, smartcards, biometrics, web access control, and electronic workflow. By selecting an existing signature-driven application, such as Travel Reimbursement, the pilot identifies and quantifies the factors contributing to a business case of replacing paper documents and manual workflow with a paperless, electronic solution that is determined and secured by digital signatures.

PLANNED PROJECT COSTS

No cost incurred. This was a free proof of concept.

EXPECTED BENEFITS

Faster transaction time, electronic history of document path, Earned trust of user community for Digital Signatures, faster reimbursement for the DMV employees, an end to end process with minimal or no paper trail, education on the use of PKI, digital certificates, Bio-metrics & I-Key technology.

STAFFING

Estimated and Actual DMV staff was: 20 Pilot participants, 1 RA, 1 network administrator, 2 Project Managers

FUNCTIONAL CONTEXT

Digital Signatures replaced the wet signatures on forms that required a supervisor or executive approval.

APPLICATION ENVIRONMENT

HARDWARE -

EXISTING [DMV]:

- Dell Latitude CPi300XT Laptop PC
- Dell PC
- Dell Monitor
- Compaq PC [Workflow Server] with existing DMV hardware/software configuration and telecommunications infrastructure

EXISTING [Unisys COE]:

- Unisys Aquanta ES [server(s)]
- Unisys EVG3100-P Monitor

New [DMV]:

- Unisys Biometric Fingerprint Reader
- GemPlus SmartCard & Reader [2]
- iKey 2000
- Hewlett Packard Scanner [2]

SOFTWARE –

EXISTING [DMV]:

- OS:
- Windows '95
- Windows '98
- Internet Explorer 5.0

EXISTING [Unisys COE]:

- OS:
- Windows NT

Baltimore Technologies

- -UniCERT v 3.1.2
- (CA/CAO/RA/RAO/Gateway)
- Oracle 8.0.5
- ValiCert - Enterprise Validation Authority
- TransIT 500
- Netscape Communicator
- Internet Explorer 5.0

New [DMV]:

- Oracle 8.0.5 (Client)
- Baltimore Technologies
- -UniCERT v 3.1.2 (RAO)
- PureEdge Viewer 4.3.1
- PureEdge/ValiCERT Plug-in
- SP I-Net AuthentiKit v 1.2
- GemSafe 1.0
- iKey 2000

Additional Server Software necessary for Electronic Forms, Workflow, and Digital Signatures via thin client:

- Windows NT Server
- Microsoft IIS 4.0
- Oracle Server Software
- Internet Explorer v 5.0
- InfoImage for NT v 4.0 or greater
- InfoImage Workflow Designer
- InfoImage Web Connector Toolkit
- PureEdge Forms Designer v 1.3
- Microsoft Visual Studio 6.0
- ValiCert Browser Plug-in

TELECOMMUNICATIONS –

EXISTING [DMV]:

- Novell GroupWise

EXISTING [Unisys COE]:

- MS Outlook

APPENDIX G

CERTIFICATE AUTHORITY

Baltimore Technologies

-UniCERT v 3.1.2

LIST OF CERTIFICATES

38 Personal Digital Certificates issued from the Unisys Security Practice Center of Excellence [Burlington, MA] to the participants of the VA DMV POC.

LIST OF PKI ELEMENTS

Certification issuance

Certificate revocation

Certification repository

Authentication

Confidentiality

Non-repudiation support

Client software

Integrity

Secure data archive

NETWORKING REQUIREMENTS

Standard DMV configuration with the exception of opening port in the current firewall to allow communications with Validation Authority.

TRAINING REQUIREMENTS

Training (completed):

DMV POC Participants –

- PKI Overview [M. Chalupa, Unisys]
- Certificate Authority Overview
    1. Downloading CA Certificate
    2. Submitting Personal Certificate
    3. Remote Request Form
    4. Installing Personal Certificate
    5. Web Access Control Enrollment
    6. Enrollment Confirmation
    7. Accessing/Processing DMV Electronic Travel Reimbursement Forms
- -Info Image Workflow for Processing
- DMV Electronic Travel Reimbursement
- Forms [Kevin Wagner, Unisys]
    1. Accessing/Processing DMV Electronic Travel Reimbursement Forms (review)
    2. Adding data to Electronic Travel Forms
    3. Applying Digital Signatures to Electronic Travel Forms
    4. Submitting, Saving, Printing, Authorizing, Adding e-Receipts to TER Forms

- DMV POC RAO (R. Fabrizio, M. Snapp)
- -RAO Functions [P. Tremer, Unisys]

1. Overview of RAO Functions
2. Starting RAO
3. Reviewing & Vetting Certificate Requests
4. Reviewing Records (Browse Event Log, Certified Users & Rejected Requests)

Training (needed) [1-2 Days]:

1. Scanning
2. InfoImage Administration
3. Submission of electronic forms in Workflow
4. Authorization of forms in Workflow

TESTING REQUIREMENTS

Elements Tested:

- -CA Functionality (CA, CAO, RA, RAO, Gateway)
- -Remote & Face-to-Face Certificate Request Operations (Personal & Server Certificates)
- -RAO Vetting of Certificate Requests
- -E-Mail Notification of Certificate Issuance & Installation Links
- -Issuing Certificates onto GemPlus Smartcards
- -Issuing Certificates onto the iKey 2000
- -Suspending & Revoking Certificates
- -Generating Certificate Revocation List (CRL)
- -Validation of Certificate Status
- -Electronic Travel Form Functionality (Applying Multiple Digital Signatures)
- -Info Image Workflow Functionality
- Workflow Route via Workflow Designer: internal validation of rules for queues, routing, and storage. High-level functional overview was developed via several meetings with DMV personnel.
- Testing of user access privileges and queues access based on functional design.
- Testing of connectivity of each user-to-user interface. All users are accessing the system via Browser (Internet Explorer 5.0)
- Internal testing of InfoImage items, i.e., custom robots, forms, queues and user privileges.
- Internal testing of WebConnector and ODBC connectivity (Oracle)
- -Scanning/Attaching Receipts to TER Form
- -Audit Functions

ACQUISITION AND INSTALLATION ACTIVITIES

Hardware:

- Hewlett Packard Scanners [2]
- acquired and installed to facilitate the scanning of travel receipts for attachment to Travel Expense Reimbursement form.
- iKey 2000

Software:

- PureEdge Viewer v 4.3.1
- ValiCert/PureEdge Plug-in
- iKey 2000

Difficulties of Installing Equipment: 431.xfd file did not always transfer to Valicert Prefs file upon installation & execution of plug-in; as a result, the preferences tab was not present in the electronic forms; this required a manual process of copying the 431.xfd file into the Valicert Prefs file on some POC participant machines.

OBSTACLES

Unisys Info Image Workflow Server could not be brought into the DMV Network; as a result, the Workflow Server had to be reconfigured using DMV equipment.

Firewall Configuration (DMV firewall rules had to be modified to allow network traffic to occur at the DMV on an outbound & inbound basis in connection with digital certificate requests, e-mail notification of certificate issuance & installation links).

CITY OF NORFOLK

By Ron Tokarcik, Information Systems Analyst

PILOT DESIGN

The City of Norfolk selected an Intranet-based Personnel Requisition System as the target application for use of digital signatures. This application was chosen for the pilot based on several criteria including the need to expedite the hiring process, which requires several signatures and manual transfer of paper documents, which slows down the overall hiring process. An internal application was preferred for this pilot to reduce the risks associated with implementing a new technology in a production environment. Additionally, the City is planning to implement other e-government applications that may require use of digital signatures. The pilot afforded the City an opportunity to experiment with this new technology that is expected to be implemented in support of Norfolk's e-government initiative.

The personnel requisition system automates the submission and processing of personnel requisitions. Once a department submits their personnel requisition via the Intranet to the Human Resources department, a personnel analyst reviews the application and begins the recruiting process. After qualified candidates are identified, the database is updated and an adobe acrobat form is created. This form is then digitally signed by the personnel analyst and routed via e-mail to the respective department. The department is then conducts the interview process to select the candidate for employment. Once a candidate is selected, the form is updated and sent to an Assistant City Manager for the next level of authorization and signature. The form is then routed back to Human Resources for hiring and payroll processing.

The project team consisting of a project lead, technical manager, functional user, programmer and telecommunication specialist worked on the project design. Initially, the City decided to work with VIPNET and Entrust (their business partner) since Norfolk had already engaged in discussions with VIPNET regarding development of e-government applications. Although, after experiencing technical difficulties with the Entrust PKI software, which was not compatible with Norfolk's, network environment, the City decided to partner with DIT and VeriSign. This decision was made after it was learned that VeriSign's PKI product was technically compatible with the City's network.

PRE-PRODUCTION

Implementation of the project involved the following steps:

- understanding the CA policies, procedures, roles and responsibilities
- conducting research on vendor products and services (Entrust, VeriSign, and Adobe)
- selection and procurement of a forms/document package supporting PKI (Adobe Acrobat)
- creation of a personnel requisition form that could be digitally signed
- installation of client software (Adobe Acrobat)
- establishing an interface with the Certificate Authority for creation and verification of signatures
- testing of application software
- training of the users

The CA established policies and procedures for security in their Certificate Policy Statement. Local security policy also includes shutting down the web browser when the user leaves their workstation. Each user is ultimately responsible for ensuring the protection of their own certificate.

No actual integration was required for this application. The system generates a Word Document form that is converted to Adobe Acrobat and routed to the users via the City's e-mail system (Outlook/Exchange Server). This document is then digitally signed and verified by the users. A number of hours have been spent by technical support staff working with the PKI vendors in addressing telecommunication issues with the CA.

PROJECT SCOPE & OBJECTIVES

The target application for this pilot is an Intranet personnel requisition system developed by the department of Information Technology. This system was implemented a year ago and has been successfully used by city departments since that time. The personnel requisition system, a web enabled database application automates the submission and processing of personnel requisitions. The system consists of a web interface used by departments to submit and review the status of requisitions and a database that records, tracks, and process requisitions. The system also generates various reports and correspondence to applicants.

Within the current process, there are two steps, which require signatures and therefore the production of a paper document. This document listing the candidates eligible for interviews ("eligible list") requires the signature of a Human Resource Team leader and once a candidate has been selected the signature of the City Manager or an Assistant City is required to indicate approval for hiring.

The pilot proposes creation of an electronic document that is digitally signed and routed via e-mail throughout the city to the appropriate individuals. This will to eliminate the need for using a paper document and manual, which delays the recruiting process.

PLANNED PROJECT COSTS

Adobe Acrobat 4.06 software for ten concurrent licenses. The total estimated cost for this software is $610 ($51 for software plus $10 annual maintenance fee for each license).

ACTUAL PROJECT COSTS

Actual costs for the Adobe software matched estimated costs. Staff time involving technical support for the project exceeded our expectations.

EXPECTED BENEFITS

Use of digital signature technology would allow for completing the automation of this process, which would result in a significant amount of time being saved in the recruiting and selection process. Additionally, Norfolk's Information Technology has already been requested by Human Resources and several other departments to find a solution that would allow for use of digital signatures.

BENEFITS OR SAVINGS EXPERIENCED

All expectations were not met since the pilot could not be fully implemented due to technical difficulties. Not having the ability to verify signatures has prevented the pilot from moving into the production phase.

STAFFING

Existing staff resources are supporting this project. The Project team consists of a Project Lead, Technical Manager, functional user who is familiar with the application and business practices, an application programmer, and a telecommunications specialist.

FUNCTIONAL CONTEXT

Used for an Internal application to support the city's hiring process. Several levels of signatures are required on the personnel requisition document used by city agencies to request positions.

APPLICATION ENVIRONMENT

The project utilized the city's existing technology infrastructure including PC workstations, local/wide area network, and Internet services.

CERTIFICATE AUTHORITY

VeriSign/DIT

LIST OF CERTIFICATES

Two certificates to Human Resource personnel (users)

NETWORKING REQUIREMENTS

The only changes made to the City's network environment were to open several ports in the firewall to allow communications with the CA.

TRAINING REQUIREMENTS

If the pilot becomes operational, training for the users will be required. Users must be able to use Adobe Acrobat to digitally sign documents and verify signatures. This training should not take more than 1 hour per user.

TESTING REQUIREMENTS

Testing completed includes certificate registration, certificate issuance and testing of the communications interface with the CA. Unfortunately, the interface with the CA is not working and thus far the problem has not been resolved. As a result, not data has been exchanged with the CA.

ACQUISITION AND INSTALLATION ACTIVITIES

Entrust client software was initially provided for pilot on a demo basis, but would not work in Norfolk's Network environment. Adobe Acrobat's full version 4.0 client software (10 licenses) was purchased by the City to support the pilot.

APPENDIX G

VIRGINIA DEPARTMENT OF TRANSPORTATION

By Ray Lindquist, Vice President of Business Systems, Parikh Advanced Systems

PILOT DESIGN

VDOT's choice of pilot application was based on previous work undertaken by the Electronic Contracting Task Force (ECTF), comprised of representatives from VDOT, Virginia Road and Transportation Builders Association, the FHWA and the contracting industry. A goal of the ECTF is to implement electronic bidding in the Commonwealth. The Goal Statement reads "To provide and encourage our contracting partners to utilize the option of submitting proposals to VDOT electronically".

Electronic bidding has been implemented in other states to various degrees. VDOT has been able to draw on the experiences of transportation departments in Georgia, Oklahoma, and North Carolina. All states are working with the same vendor, InfoTech, Inc., a company that has developed many of the systems, e.g. Trns*port, in use by transportation departments across the nation.

The process begins by the creation of an electronically distributable file produced by Expedite from existing Trns*port data. The file is unique for each advertised project and is made available on a web server for contractors to download to their own computer system.

Each potential signer within a contracting firm is required to create a key pair (two key pairs, one for signing and one for encryption) using the Expedite software. The public part of the key pairs is submitted over the Internet to the Bid Express service, and is also printed on a “digital ID request” form. The signer must sign the form, have it notarized, and return the physical form to InfoTech before the key is activated. The ID request form also contains legal language that binds the signer to be responsible for use of his keys. The contractor then uses a free version of the Expedite software to complete, sign, and securely encrypt the unit price portion of their proposal.

Prior to the bid deadline the contractor submits the electronic proposal to a system of servers designed to securely hold the data until the bid period expires. Following the deadline, VDOT retrieves the secured data from the servers and begins processing the data. Once the results are compiled the bids are read publicly. Avoiding the current practice of keypunching, the data is electronically transferred into the Department’s Trns*port system to be prepared for award.

PRE-PRODUCTION

The Electronic Contracting Task Force (ECTF) developed an aggressive implementation schedule for the electronic bidding pilot. Communications between ECTF members were organized on the ECTF web site and included an access-controlled discussion web. Initial tasks revolved around communications with InfoTech and placement of a generic version of Trns*port on VDOT's test region by the Agency's Information Technology Division.

The Virginia Road and Transportation Builders Association (VRTBA) Engineer Director led the effort to promote the e-bidding concept to members of the contracting industry and to solicit volunteers for a first mock letting. Five contracting firms volunteered for the initial letting with an additional four signing up for the second mock letting.

Volunteer contractors and VDOT staff members received training by InfoTech on the use of Expedite software and key generation. VDOT staff received training on use of InfoTech's Bid Express Retrieval Console (BERC), used to retrieve bids from Bid Express servers following bid deadline.

Survey questionnaires for contractor participants were developed by the ECTF and InfoTech. These were used to measure the degree of satisfaction of users of the system and recording of any problems experienced during bid submissions. Problems encountered were forwarded to InfoTech and received immediate attention. Suggestions for product improvements were made by the ECTF team. These received favorable attention from InfoTech and will be included in future releases of Expedite.

Existing policies and procedures were reviewed and deemed acceptable for the initial pilot mock lettings. Policies in effect other states where paper bids take precedence over electronic bids were considered. No decision has been taken in this regard at the time of writing. Future policies relating to bid submission on disk will be developed if the Department decides to allow this bidding option.

PROJECT SCOPE & OBJECTIVES

Initial mock letting; July 7, 2000
Second mock letting with larger group of contractors: August 11, 2000
Pilot with 2 lettings; September 1 - October 30, 2000
Proposed full implementation: November 2000

PLANNED PROJECT COSTS

Two Service Units from VDOT's contract with InfoTech = $ 25,000

ACTUAL PROJECT COSTS

$ 25,000

EXPECTED BENEFITS

- Reduction of errors for VDOT and contractors reduces number of re-advertisements.
- Reduction in expenditures on paper, filing and handling costs, postage, and data storage.
- Elimination of keypunch requirements results in a faster contract award process.
- Electronic bidding will be voluntary and therefore will not exclude firms with limited resources from bidding in the traditional method.

BENEFITS OR SAVINGS EXPERIENCED

Following two instances of electronic bidding on mock lettings all anticipated benefits have been experienced. Savings are not quantifiable at this very early stage.

STAFFING

Staffing included members of previously established Electronic Contracting Task Force (includes 12 VDOT staff, 1 representative from FHWA, and 5 from contracting industry) two additional VDOT staff members providing expertise on Trns*port system, and one Data Management Division staff member acting as liaison to COTS DSI workgroup.

FUNCTIONAL CONTEXT

VDOT utilizes an existing system, Expedite, developed by InfoTech, Inc. that is designed to work with AASHTO's Trns*port system. The process closely parallels system currently in production in Georgia, South Carolina and several other AASHTO member states. VDOT already licenses and uses Trns*port to build and maintain contract data and therefore owns the Expedite license.

The process begins by producing an electronically distributable file produced by Expedite from existing Trns*port data. The file is unique for each advertised project and will be available on a web server for contractors to download to their own computer system. The contractor then uses a free version of the software to complete, sign, and securely encrypt the unit price portion of their proposal.

Prior to the bid deadline the contractor submits the electronic proposal to a system of servers designed to securely hold the data until the bid period expires. Following the deadline, VDOT retrieves the secured data from the servers and begins processing the data. Once the results are compiled the bids are read publicly. Avoiding the current practice of keypunching, the data is electronically transferred into the Department's Trns*port system to be prepared for award.

APPENDIX G

PROJECT PLAN

http://www.vrtba.org/ectf/mockletting/VDOT-DSI-Pilot.mpp

CERTIFICATE AUTHORITY

Each potential signer is required to create a key pair (two key pairs, one for signing and one for encryption) using the Expedite software. Keys are issued by the Expedite BID program during the self-administered creation of a Digital ID. This is achieved through the use of a "Digital ID Wizard" and includes recording random mouse movements during a short time period. The public part of the key pairs is submitted over the Internet to the Bid Express service, and is also printed on a “digital ID request” form. The signer must sign the form, have it notarized, and return the physical form to InfoTech before the key is activated. The ID request form also contains legal language that binds the signer to be responsible for use of his keys.

InfoTech manages all keys internally, and verifies the digital signatures directly (known as the “referral” approach to verification, as opposed to a certificate based “directory” method). Contractors contact InfoTech to revoke keys as needed. A contractual agreement between InfoTech and VDOT covers the verification of the signatures.

In brief, VDOT would not verify the digital signatures, instead it would receive InfoTech’s verification of the signatures.

Added security is taken by InfoTech to verify that the requestor of a digital key is an employee of the contractor stated. This verification by InfoTech involves a call to the contractor using the contractor's pre-qualification telephone number on VDOT's vendor file. This ensures fraud does not enter the process.

LIST OF PKI ELEMENTS

Authentication

Confidentiality

Key backup

Key recovery

Secure time stamping

Client software

Notarization

Secure data archive

NETWORKING REQUIREMENTS

No changes to the existing network were necessary.

TRAINING REQUIREMENTS

Internal Procedural Training – Training of VDOT personnel responsible for the preparation and processing of the electronic bid files was required. These procedures are similar in function to the current practice of preparing the bid and award files in the Trns*port system.

Industry Training – One of the most important items to ensure acceptance of this system is proper training of the contracting industry. Through numerous demonstrations and hands-on training contractors were shown the simplicity, reliability, and advantages of the new method of bidding. An important facet of the training lies in the handling of digital keys and passwords in a secure manner. This was emphasized during training.

It will be necessary to continue periodic promotional and training opportunities once the system is in production.

Desirable pre-requirements include: General knowledge of the Windows environment, saving, re-naming, and printing of files, ability to navigate the Internet using a web browser.

Outline of training sessions held on August 7th and 8th:

Monday August 7th at the Training Center

8:00-12:00 DOT Bid Express/Expedite Train the Trainer/System Manager Training

Bid Express User Training
Bid Express System Admin Training
Expedite Bid Training
Expedite System Managers Training

2:00PM - 4:00 PM Contractor Bid Express/Expedite Training

Bid Express User Training
Expedite Bid Training

Tuesday August 8:00 at VDOT

08:00- 2:30 PM Bid Express-Expedite Customization/Configuration discussions

PGP Key creation and management Training
Bid Archive procedures

TESTING REQUIREMENTS

- Export of proposal from Trns*port - OK with generic code. Expected to be resolved and released into production late August, 2000.
- Bid submission
- Bid re-submission, overwrite of previous bid
- Bid submission by holder of 2nd ID
- Bid withdrawal
- Encryption of bid amounts
- Time-stamping of bid
- Signature key back up
- Bid submission after deadline - not allowed
- Bid retrieval before deadline - not allowed by system
- Retrieval of bids and download into BERC
- Import into Trns*port
- Saving bid submission to disk and importing into Trns*port (optional bid submission method used in other states)
- Electronic bids compared to faxed copies - identical.
- "Certificate" content verification against vendor information in Trns*port
- Bid options
- Bid revisions
- Bid delay with submission before delay and attempted submission after delay
- Stress testing of Bid Express server through bid submission by entire test group at same time
- Account spoofing through submission using other person's vendor ID and password

APPENDIX G

DEPARTMENT OF GENERAL SERVICES

By Jan Fatouros, Director of Information Systems & Services and Angela Norville, DPS Web Coordinator

PILOT DESIGN

Selection of DGS' digital signature pilot required balancing business process assessment/re-design opportunities and technology learning opportunities. During the selection process DGS identified several labor and paper intensive processes that could be facilitated through the use of electronic forms and digital signatures. We then determined business staff resource capabilities and commitment, the ease of understanding the current process, barriers to implementation (policy, practice, or legal) and conducted an abbreviated feasibility assessment of the candidate processes.   From the technology perspective, we wanted to limit our solution options to commercially available products. Ideally, the selected forms package would require limited or no programming experience, have large market penetration, and be delivered enabled to use and validate a digital signature certificate. Additional considerations were the ease of extracting data from the form, integration with our web-based document management system and features that would provide an appropriate audit trail/paper-based documentation.

The beginning and concluding tasks of the spot bid procurement process within the Division of Purchases & Supply (DPS) were selected. Reasons for focusing on these tasks included the limited length of time for the pilot, identification of where a signature was mandatory, and avoidance of code and policy barriers. The spot bid process is initiated when an agency sends an Agency Purchase Request Form (APR) to DPS. These forms are reviewed for completeness, an authorized signature (which commits agency funds), and commodity classification. Once these tasks are completed APR information is entered into a tracking system, and then forwarded to the purchasing supervisor responsible for the commodity. The supervisor reviews the APR and assigns the request to a DPS buyer for processing. The buyer then reviews the requests, develops specifications and begins the solicitation process. Once a vendor is selected, the digital signature pilot resumes with the notice of award and issuance of a purchase order that were both digitally signed. The award notice is posted on the DPS web site, and the digitally signed purchase order is sent, via e-mail to the winning vendor.

Three forms were developed to support the pilot: Agency Purchase Request, Notice of Award, and DPS Purchase Order. Adobe Acrobat 4.0 was used to develop and process the forms. The Division of Purchases and Supply developed the initial forms and established the input fields. Information Systems continued the development process by placing edits and data formats on fields, inserting the digital signature field, and validated that field-locking actions executed correctly. The forms were then reviewed in a joint session with DPS end-users to ensure the forms conformed to business practice. Additions required to the forms included adding fields for notes and corrections. Digitally signing a form establishes a baseline for validation, therefore any modification to the form causes a notification that the form has been changed.   Within DPS it was common practice for the staff to correct the form as it was processed. In a paper process this was achieved by pen and ink changes. The digital equivalent of this was to allow for notes and fields that could be digitally signed by the reviewer. During the review, we also determined that the bid tabulation sheets generated by the DPS spot purchasing system and the purchase order generated by the system should be used in place of the forms. To accommodate this requirement, the electronic reports generated from the system were converted to Adobe PDF files and then digitally signed. This modification was easy for the end users and streamlined processing of the Notice of Award and Purchase Order.

Adobe Acrobat 4.0 was chosen for the pilot because Adobe provided a plug-in for Entrust digital signatures, DPS used Adobe Acrobat for posting on the DPS web site, and many of our customers (agencies and vendors) already had the Adobe reader installed. We did not know when we made this selection that to validate a signature vendors would require Adobe Acrobat, not just the free Adobe Reader, and that extensive programming was required to extract data from the forms.

To manage the issuance of digital certificates a DPS coordinator was designated. The coordinator selected division, agency, and vendor users to participate in the pilot. The coordinator emailed a digital signature request to the DGS security officer for registration. The request included user name, organization, and email address.

PRE-PRODUCTION

The tasks required for production included approval of a digital signature security policy and end-user pilot agreement, development and testing of the forms, documentation of the existing and proposed business process, selecting pilot users, training, digital signature registration, and software distribution. A team of DPS buyers, managers and administrative staff selected candidate agencies and vendors, developed the security/registration policy, and evaluated the forms. They also were responsible for tracking processing time, determining documentation controls, and providing lessons learned.

To place the pilot in production, each user required installation of Adobe Acrobat 4.0, an Adobe plug-in to enable use of Entrust certificates, Entrust Entelligence 5.0 client software, a copy of the forms, and a signed demonstration pilot agreement. . The DPS coordinator reviewed software requirements with each user, created a package of instructions and required software, forms, and the pilot agreement. The installation package was expressed delivered to off-site users and hand-delivered to on-site users. Once the pilot agreement was signed and returned to the coordinator, she assisted the users with software installation, and provided the user the reference and authorization codes. On-site users followed a similar procedure, except the DPS coordinator installed the software. After software installation, the DPS coordinator reviewed the security policy for maintaining the digital signature, provided one-on-one training on the use of the forms, and requested that each user send a digitally signed set of test forms to her. After successful completion of the test, users then began digitally signing documents. Installation and training required 2-3 hours per user.

Installation was made time-consuming by a number of factors. In some instances old versions of Adobe needed to be removed prior to installing Adobe 4.0. Many of our users used dial-up connections to access the Internet. A connection to the Internet was required before the Entrust software could be successfully installed. User PC expertise greatly affected the time required installing software and establishing the digital signature. Using digital certificates with forms requires plug-in software to be copied into specific desktop directories; this task proved particularly challenging for some off-site users. Other unanticipated problems included users inadvertently encrypting documents, e-mailing digitally signed documents to users that could not read the mail, and keyboard number locks and shift locks being active during installation.

Costs for software was $300 per user for 10 production users. This cost was avoided by negotiating free use of the software for the pilot. Technical time required to establish, test, and document required 80 man-hours. Installation and training 30 hours with on-going support for the end-users requiring one hour per day during the pilot period. Problem investigation, resolution, and research consumed approximately 180 man-hours. Research hours included determining how to extract data from the Adobe form for update into the spot purchasing application. After extensive review, ISS determined too much unbudgeted programming work would be required and dropped data upload from the pilot. Also, understanding how digital signatures worked with GroupWise E-mail required considerable investigation. The final resolution was that digitally signed e-mail and encrypted e-mail worked fine within the DGS environment for pilot users with Entrust software. It did not work at all when mail was digitally signed and sent to users without Entrust software loaded. DGS also attempted to use other X.509 certificates with GroupWise, those certificates could not be interpreted by the Entrust/GroupWise client.

DGS functional users in the Division of Purchases and Supply actively participated in the pilot. They spent 50 hours assisting in development of the forms and reviewing the re-designed process, and developing registration policies, 45 hours in installation and support activities, 50 hours on product evaluation and experimentation, and 120 hours in pilot execution activities.

PROJECT SCOPE & OBJECTIVES

Purpose: To evaluate the use of a managed certification authority and digital signatures in the state procurement process.

Objectives**:** Determine appropriate uses of digital signatures for procurement constituencies: suppliers and buyers

- Establish an organized approach for the management of certificates that insures the integrity of the certificates and provides a common experience for suppliers & buyers in their public and commercial digital signature transactions.
- Provide an opportunity for state procurement offices to learn about digital signatures and appropriate uses within the procurement process
- Provide information about cost/benefit estimates for statewide adoption of digital signatures in procurement transactions
- Implement a security solution, that supports open standards and uses commercially accepted technologies.

Scope: DGS will target two constituencies during the pilot suppliers and agency buyers. In the initial phase the DPS Purchase Requisition form will be electronically submitted to DGS/DPS by selected state agencies. The form will use digital signatures in place of the required agency authorized signature. DPS buyers will utilize digital signatures on "Notice of Contract Award" documents that will be posted on the DGS Procurement Web site and e-mailed to suppliers.

In the second phase DGS/DPS developed a Purchase Order e-Form that supported digital signatures. Trading agreements will be executed with key suppliers to accept digitally signed purchase orders.

PLANNED PROJECT COSTS

Software: $5,000 Staff time: $20,000

ACTUAL PROJECT COSTS

Functional Time $9,500 (meetings, training, testing, executing pilot)

Technical Time $11,000 (meetings, establish environment, resolve technical issues, development of process)

Software for pilot was donated

EXPECTED BENEFITS

Reduced forms processing time. Reduced staff administrative time.

BENEFITS OR SAVINGS EXPERIENCED

Intangible benefits:

- Improved authentication of signatures
- Improved control on form changes/corrections
- Reduces document travel time to intended recipient by 7 days.
- Reduces contract travel time to vendor 15 minutes – 3 days (fax-mail).

Tangible benefits

- Labor savings: 75 minutes per contract (scanning of signed contracts for posting on web sites)

STAFFING

Nine technical and business process staff. We added four additional support staff. Two within DPS to coordinate and support use of digital signatures. One to work through detail forms development issues within ISS.

FUNCTIONAL CONTEXT

Create Standard Procurement Forms with digital signature capability. Our intent was to reduce forms travel time and administrative time in posting signed documents to our web site.

APPLICATION ENVIRONMENT

EXISTING

Hardware:

- Dell Pentium II PC on each desktop
- Dell dual processor web server

Software:

- Window 97 Desktop Operating System
- Internet Explorer 5.0
- Adobe Acrobat 3.0
- Adobe Acrobat Reader
- Web Server –IIS and Windows NT 4.0
- GroupWise Email 5.0

ADDITIONS:

- Adobe Acrobat 4.0 with Entrust Ad-on
- Entrust Entelligence 5.0

CERTIFICATE AUTHORITY

VIPNet.

LIST OF CERTIFICATES

Fourteen certificates were issued.

LIST OF PKI ELEMENTS

Certification issuance
Authentication
Non-repudiation support
Client software
Integrity
Privilege/policy verification

NETWORKING REQUIREMENTS

No changes were made to the network. We did need to enable two ports on the DGS firewall. This allowed certification issuance and authentication verification of certificates issued by the VIPNet Certification Authority. The ports that must be enabled are Port 829 for client to CA access and Ports 709/710 for CA to Agency network access.

TRAINING REQUIREMENTS

DGS received no vendor training on any of the products used in the pilot. Training on developing forms in Adobe particularly in data extraction would have been extremely helpful. Training by a qualified person on Entrust Client Software would have greatly assisted installation and resolved initial problems with the software and aided understanding of how to use the software. DGS did install a pilot PKI laboratory with the assistance of Parikh Systems, which greatly assisted DGS technical staff in understanding PKI concepts. DPS developed an installation guide for the Entrust software and provided a brief one-on-one demonstration for each user on how the product worked.

TESTING REQUIREMENTS

- Registration and certificate issuance,
- Infrastructure testing with the CA
- Simulation run through the entire process
- Connectivity functions (encryption and decryption)
- Use of test data to validate data exchange.

ACQUISITION AND INSTALLATION ACTIVITIES

Entrust Entelligence 5.0 for each client was provided by the vendor for the demonstration.

OBSTACLES

It is very difficult to issue a certificate to a dial-up user. If it is a single user on a dedicated modem then the issue can be easily resolved by having the user establish an internet connect prior to beginning the installation. For users that share a pool of modems off a network, it appears that the connection is dropped during the time it takes to install the software, making a smooth installation of the software and certificate difficult. For one vendor, we abandoned the test because a connection to the CA could not be established.

Lack of basic PC skills was another obstacle. For most of our users the installation was too difficult to successfully perform with only checklist instructions. We discussed developing an installation script to automate removal of Adobe 3.0, installation of Adobe 4.0, movement of the Entrust Adobe plug-in to the correct directory and then installation of Entrust. Lack of installation standards for the target pilot users made this approach overly complex for the pilot.

GroupWise client software requires enhancement packs to work optimally with X.509 certificates. Based on our review of problems the enhancement packs could cause with other mail functions, we decided not to install enhancement packs to our GroupWise clients.

Using a forms package requires each user have the forms package. This is both a cost and compatibility obstacle. If fill-in forms are used, COVA needs to set a standard for citizen forms. We were also surprised by the complexity in data extraction from the forms. Our assumption was that the forms would have an export utility. This is not the case. To interface the forms package with an agency database requires field-level programming in visual basic or java.

UNIVERSITY OF VIRGINIA (THE BRIDGE)

By Tim Sigmon, Director of Advanced Technology; Chip German, Director of Planning & Policy Development; and Shirley Payne, Director of Security Coordination & External Relations

PILOT DESIGN

The objectives of this pilot project were to:

1. demonstrate the adaptability of the federal PKI bridge architecture and other federal approaches to the Commonwealth's PKI implementation, and
2. simplify the Commonwealth's PKI environment by providing common requirements for interoperability through the bridge while maintaining each agency's choice in determining which certificate-based solution(s) is (are) right for it.

The second objective is especially critical for state agencies, such as higher education institutions, that have need to interoperate with entities outside the realm of Virginia state government.

The scope of this project included establishment of a Commonwealth of Virginia PKI Bridge that allowed pilot PKI applications to rely on certificates issued by varied sources in establishing the identity of users (individual or group).

During the pilot phase, the bridge employed mainly manual mechanisms for issuing cross-certificate pairs and using them to establish a trust relationship between a user in one trust domain and a relying party or relying application in another trust domain. Use of the Bridge, from an end-users perspective, is transparent.

A demo application was developed to illustrate the correct operation of the bridge architecture. The application exists in one trust domain and is capable of accepting and verifying digitally signed web forms from users who exist in a different trust domain. This demo can be viewed at http://atg2000.itc.virginia.edu/BridgeDemo.

A major assumption of the bridge architecture is that applications will establish authorization levels for users -- the bridge will assist in verifying a digital signature (the identity of the signing party and the integrity of the signed document), not what the signing party is authorized to do. Our conversations with vendors confirm our impression that the elimination of authorization information from digital signatures simplifies the implementation of PKI to a highly desirable degree.

Open source software was used to establish the Bridge because it provided all the functionality that was required, it was immediately available, and it could be obtained free of charge. The open source software also allows technical staff a much clearer understanding of how the functions of various components of PKI are accomplished and allows them to modify the source code if such a step is needed for particular implementations.

PRE-PRODUCTION

Provide a brief summary of the implementation strategy and the steps taken to put the pilot into production. Please include information on policies and procedures, roles and responsibilities, application integration, and time and funds expended.

The pilot BCA is based on the open source packages OpenSSL (http://www.openssl.org) and OpenCA (http://www.openca.org) running on RedHat Linux version 6.1. The BCA machine itself can remain turned off most of the time in a secure location and only needs to be booted upon receipt of a request for cross-certification. Once it has created the cross-certificate, it can again be turned off. Typically, when the BCA cross-certifies with another CA, there will actually be two certificates created, one in which the BCA is the issuer and the other CA is the subject and one in which the other CA is the issuer and the BCA is the subject. Since cross-certifications are relatively infrequent events, the process of getting a request, creating the signed certificate, and exporting the certificate can be a fairly manual process. This is particularly true for Virginia’s pilot BCA project.

The profile of the cross-certificates created by the pilot BCA was modeled after the profile being used in the federal bridge project, see http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls. The cross certificates themselves can be viewed at http://atg2000.itc.virginia.edu/BridgeDemo.

Since the cross-certificates carry public information and are integrity protected (i.e., any change to the certificate will be detectable due to the digital signature), they can be distributed and shared by any and all means. For example,

- Distribute via floppies or other removable media
- Distribute via email
- Publish via web sites
- Publish via directories (e.g., LDAP, X.500) using the crossCertificatePair attribute which stores the forward and reverse certificates together

Ultimately, distribution via directories needs to be in the solution set. However, for the pilot project, this was not necessary.

Certificate path processing and signature verification need to be performed by the relying parties, and the relying parties are determined by the application types. For example, if the application involves the use of digitally signed email messages, all potential recipients would need to be able to perform path processing and signature verification. Currently, most email packages that have the ability to verify a digital signature can only do so in a hierarchical environment, not one in which cross-certifications are involved (although a special version of Eudora with this capability was produced as part of the demonstration of the Federal BCA).

However, if the application involves the use of digitally signed transactions or documents such as web-based forms that are submitted to a central location, then the requirement for being able to verify digital signatures is restricted to the back-end or server-based application software.

APPENDIX G

For the purposes of the Virginia bridge pilot project, we illustrated the usefulness of a bridge architecture by employing applications that require digitally signed forms, since it's much easier to deploy the necessary software for verifying digital signatures that occur in a cross-certification environment in this more restricted server-based environment. UVa developed such a demonstration using web-based forms and built into the application the ability to perform certificate path construction in a cross certification environment.

During the prototype, roles were assigned to UVa participants as appropriate. Professional time was donated and hardware was loaned for this project by the University. Approximately 6 person months of effort were devoted to design and establishment of the Bridge. The University has contributed additional time, estimated at 5 person months, to actively participate in the overall DSI effort.

PROJECT SCOPE & OBJECTIVES

The objectives of this project were to:

1. demonstrate the adaptability of the federal PKI bridge architecture and other federal approaches to the Commonwealth's PKI implementation, and
2. simplify the Commonwealth's PKI environment by providing common requirements for interoperability through the bridge while maintaining each agency's choice in determining which certificate-based solution(s) is (are) right for it.

The second objective is critical for state agencies, such higher education institutions, that have need to interoperate with entities outside the realm of Virginia state government.

The scope of this project included establishment of a Commonwealth of Virginia PKI Bridge that allowed pilot PKI applications to rely on certificates issued by varied sources in establishing the identity of users (individual or group). Eventually the bridge architecture will need to involve many automated processes. During the pilot phase, however, the bridge employed mainly manual mechanisms for issuing cross-certificate pairs and using them to establish a trust relationship between a user in one trust domain and a relying party or relying application in another trust domain. A major assumption of the planned bridge architecture is that applications will establish authorization levels for users -- the bridge will assist in verifying a digital signature (the identity of the signing party and the integrity of the signed document), not what the signing party is authorized to do.

This project also included drafting proposals in concert with the DSI for overall management of a Commonwealth of Virginia public-key infrastructure that incorporates a cross-certification bridge and of the bridge architecture.

PLANNED PROJECT COSTS

No incremental costs were expected.

ACTUAL PROJECT COSTS

No incremental costs were incurred. The University donated professional staff time and existing hardware to the project.

EXPECTED BENEFITS

Use of bridge architecture within the Commonwealth will allow individual agencies to implement digital signature solutions that meet their specific needs, without compromising their ability to interoperate with PKI solutions of other state agencies and entities outside Virginia state government.

By keeping authorization at the application level, rather than embedding authorization information in certificates, modification of authorizations can be accomplished without reissuing certifications. In the case of vendor solutions that charge based upon the number of certificates issued, there should be tangible cost savings realized with this approach.

BENEFITS OR SAVINGS EXPERIENCED

All expectations were met.

STAFFING

Four UVa staff members worked on the Bridge Project. Work consisted of technical architecture design, software development and testing, and policy development and was performed by existing staff.

FUNCTIONAL CONTEXT

This project included establishment of a Commonwealth of Virginia PKI Bridge that allowed pilot PKI applications to rely on certificates issued by varied sources in establishing the identity of users (individual or group). During the pilot phase, the bridge employed mainly manual mechanisms for issuing cross-certificate pairs and using them to establish a trust relationship between a user in one trust domain and a relying party or relying application in another trust domain.

APPLICATION ENVIRONMENT

The development and operations environment consists of Linux running on Wintel hardware platforms, Open Source software, Java, and normal connections to the Internet.

CERTIFICATE AUTHORITY

UVa served as the Bridge CA using Open Source software

LIST OF CERTIFICATES

Cross certificate pairs were issued between the bridge CA and several test CAs for the purpose of demonstrating the bridge certification architecture via an application that employed digitally signed web forms.

LIST OF PKI ELEMENTS

Certification issuance
Certificate revocation
Certification repository
Cross-certification
Authentication
Non-repudiation support
Privilege/policy creation
Key history management
Client software
Integrity
Privilege/policy verification

TESTING REQUIREMENTS

Functions tested:

- bridge CA issued cross certificates
- developed and tested an application that exists in one trust domain and can accept/validate digitally signed web forms from a user in a different trust domain.

ACQUISITION AND INSTALLATION ACTIVITIES

OpenSource software was downloaded from the Internet. Existing Wintel hardware platforms were being used. Demo application was developed in house. No difficulties were encountered.

OBSTACLES

We encountered problems in how the current browsers support the management of digital credentials. Also, off-the-shelf policies that governed the DIT PKI implementation using VeriSign prevented us from fully demonstrating cross-certification between Entrust (VIPNET and DGIF) and VeriSign certificates. However, we were able to accomplish one-way cross-certification that allows VeriSign or Entrust certificates issued by DIT or VIPNET or DGIF to interact with UVa's web application. These issues are more fully explained in Part Two of this report.

APPENDIX H

COMMONWEALTH BRIDGE CERTIFICATION AUTHORITY

By Tim Sigmon, University of Virginia

August 8, 2000

BACKGROUND ON TRUST MODELS AND JUSTIFICATION FOR A BRIDGE CA

When using digital signatures in a PKI, the relying party or application exists in a trust domain that defines the set of certificates that it is able to verify and trust. In practice, this means that the relying party or application has access to one or more “root” or self-signed certificates that it trusts (for reasons outside the scope of the PKI). In the most common case, these root certificates are used to verify the authenticity of a hierarchical chain of certificates that were involved in a digital signature. In this simple hierarchical structure, the only certificates that can be used for digital signatures with this application or relying party are those that were issued by CAs verifiable by one of these trusted roots, i.e., CAs that exist in one of those trusted hierarchies. In the simplest case, the trust domain could be that of a single CA. In other cases (e.g., the browsers distributed by Netscape and Microsoft), there may be an extensive list of trusted CAs, which means that certificates issued in any of those hierarchies would be verifiable and therefore trusted.

A major problem with this hierarchical model of trust relationships among CAs is that if the private key of the root CA is compromised, the entire hierarchy of CAs and end entity certificates collapses. Another problem is related to the need for each application or relying party to have to decide for itself which root certificates, i.e., which trust domains/hierarchies, it will trust and for what reasons. In practical terms, this is further complicated by the need to employ some “out-of-band” mechanisms to securely distribute these root certificates since their integrity is not protected by their own signature. Even after securely acquiring a number of root certificates (representing a number of hierarchies), one must continually ensure that this “trust list” is not inappropriately altered to include CAs that should not be on the list. A much simpler environment would exist if each application or relying party could establish one root CA (or a small number) that it trusts and not be required to continually add more root CAs in order to expand its trust domain.

This is where the notion of cross-certification comes into play. Cross-certification is a technically simple process whereby CA A and CA B sign each other’s public keys creating two certificates that are called a cross-certificate pair. With these in place, an application or relying party in the trust domain of CA A can verify a digital signature created via the corresponding private key of a certificate that was issued by CA B (or one of its subordinate CAs). This is possible since the application can trace the certificate chain of trust all the way from the signing certificate to the application’s own trusted root certificate by using the appropriate cross-certificate.

Cross-certification between CAs allows a particular application or relying party to enjoy the benefits of an expanded trust domain without being required to exist in the same trust hierarchy as the other domains (and suffering the previously described risks). With cross-certification, if one of the hierarchies with which a particular CA has cross-certified collapses, then the CA in question can continue trusted operation within its own hierarchy as well as with all other non-compromised cross-certified hierarchies. Also, the number of root certificates obtained and managed by relying parties can remain small while still operating in an expanded trust domain.

A potential issue with this cross-certification model is that the number of cross-certifications required grows as n^2 if a collection of n CAs wish to interoperate with each other, i.e., applications or relying parties in one CA’s trust domain want to be able to accept and verify certificates from all the other CAs’ trust domains. This is sometimes referred to as a completely interconnected cross-certification mesh.

It is this n^2 cross-certification problem that is addressed by the bridge CA (BCA) architecture. With a BCA in place, each CA needs only to cross-certify with the BCA in order to expand its trust domain to include those of other CAs which have also cross-certified with the BCA.

APPENDIX H

TECHNICAL AND OPERATIONAL ISSUES FOR THE BCA

The pilot project led by the University of Virginia has demonstrated the efficacy of the BCA architecture for the Commonwealth of Virginia. The pilot BCA is based on the open source packages OpenSSL (http://www.openssl.org) and OpenCA (http://www.openca.org) running on RedHat Linux version 6.1. The BCA machine itself can remain turned off most of the time in a secure location and only needs to be booted upon receipt of a request for cross-certification. Once it has created the cross-certificate, it can again be turned off. Typically, when the BCA cross-certifies with another CA, there will actually be two certificates created, one in which the BCA is the issuer and the other CA is the subject and one in which the other CA is the issuer and the BCA is the subject. Since cross-certifications are relatively infrequent events, the process of getting a request, creating the signed certificate, and exporting the certificate can be a fairly manual process. This is particularly true for Virginia's pilot BCA project.

The profile of the cross-certificates created by the pilot BCA is modeled after the profile being used in the federal bridge project (*http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls*). Examples of these cross-certificates can be viewed at *http://atg2000.itc.virginia.edu/BridgeDemo*.

Since the cross-certificates carry public information and are integrity protected (i.e., any change to the certificate will be detectable due to the digital signature), they can be distributed and shared by any and all means. For example,

- Distribute via floppies or other removable media
- Distribute via email
- Publish via web sites
- Publish via directories (e.g., LDAP, X.500) using the crossCertificatePair attribute which stores the forward and reverse certificates together

Ultimately, distribution via directories needs to be in the solution set. However, for the pilot project, this was not necessary since the cross certificates were easily cached with the demo application (digitally signed web forms).

ISSUES FOR APPLICATIONS OR RELYING PARTIES

The relevant activity that applications or relying parties need to be able to perform is to verify the digital signatures on incoming documents or transactions. This activity can be broken into three phases: certificate path construction, certificate path validation, and signature verification. The first two phases, sometimes referred to as certificate path processing, determine whether the signer's public key can be trusted before it is used for the cryptographic operations involved in verifying the signature.

Certificate path construction. Certificate path construction involves gathering all the certificates necessary to form a trust path from the signer's certificate to a trusted root certificate (i.e., a self-signed certificate). In a strictly hierarchical environment, certificate path construction is a straightforward process whereby the application or relying party simply follows the chain of issuers starting from the certificate of the signer to one of its trusted roots. Currently, the two popular browsers, Netscape Navigator and Microsoft Internet Explorer, have the built-in capability to verify digital signatures in a hierarchical environment. Also, a number of popular email packages have this ability since they support the S/MIME standard for digitally signed email messages (e.g., Netscape Messenger, Microsoft Outlook Express, Eudora).

Certificate path construction in an environment involving cross-certifications (whether a bridge architecture is employed or not) is potentially a much more difficult process. The goal is still to construct a path starting from the certificate of the signer to a trusted root, but now there may be many possible paths.

Cygnacom Solutions (http://www.cygnacom.com) has developed a Certificate Path Development Library (CPL) that is freely available and is protected by the Mozilla Public License (MPL), version 1.1. The CPL can discover all possible paths from an entity certificate to a trusted root and will return them in a prioritized order based on heuristics that order them from most likely to be verifiable to least likely. The CPL does not provide code to obtain and/or cache the needed certificates, but instead provides callouts for this activity.

For Virginia's pilot bridge project, acquisition of the necessary certificates was simplified by manually caching all relevant cross-certificate pairs in the applications or relying parties, thus making path construction a bit easier and obviating the need for directory services. Ultimately, of course, the needed certificates should be obtained from LDAP directories or from a cache of previously obtained certificates. In addition, the pilot demonstration application was enhanced to be able to construct certificate paths using these cached cross-certificates.

Certificate path validation. Certificate path validation involves examining each certificate in the path to determine whether or not the contained key can be trusted. This activity is the same whether dealing with a strictly hierarchical trust environment or one involving cross-certifications. Briefly, for each certificate, one needs to:

- Verify the digital signature
- Check the validity period to ensure that it was valid at the time the transaction/document was signed
- Check the revocation status via CRLs and/or OCSP to ensure that it was valid at the time the transaction/document was signed
- Check any applicable policies, key usage restrictions, name constraints, etc.

A successful validation of the certificate path means that the signer's certificate can be trusted, i.e., the binding between the signer's identity and their public key is valid and the integrity of the public key is assured.

Signature verification. Now that the signer's public key is known to be trustworthy, the digital signature that was applied to the original incoming document or transaction can be verified. This involves the following steps:

- Use the signer's public key to decrypt the message digest that was computed by the signer
- Compute a message digest of the received document or transaction
- If the two message digests are equal, then the signature is valid (i.e., the signer's identity is validated and the integrity of the document or transaction is assured

PILOT PROJECT APPLICATION

To re-emphasize, certificate path processing and signature verification need to be performed by the relying parties, and the relying parties are determined by the application types. For example, if the application involves the use of digitally signed email messages, then all potential recipients would need to be able to perform path processing and signature verification. Currently, most email packages that have the ability to verify a digital signature can only do so in a hierarchical environment, not one in which cross-certifications are involved (although a special version of Eudora with this capability was produced as part of the demonstration of the Federal BCA).

However, if the application involves the use of digitally signed transactions or documents such as web-based forms that are submitted to a central location, then the requirement for being able to verify digital signatures is restricted to the back-end or server-based application software.

For the purposes of the Virginia bridge pilot project, the usefulness of the bridge architecture was illustrated by developing a simple application that required a digitally signed web-based form. This type of application was chosen since it's much easier to deploy the necessary software for verifying digital signatures that occur in a cross-certification environment in this more restricted server-based environment.

APPENDIX H

QUICK SUMMARY OF ASSUMPTIONS AND ISSUES

- A number of simplifying assumptions were made for the pilot:
  - Focus on applications in which the relying parties are centralized rather than distributed. For example, form/document signing and submission to a server-based application rather than signed email among a large population.
  - Manual distribution of cross-certificates to obviate the need for directories.
  - Keep policy mapping issues to a minimum by using CAs with identical (or at least compatible) policies.

- The pilot bridge CA was based on open source and freely available software running on a Linux machine.

- Signature verification software was enhanced to work in a non-hierarchical environment involving cross-certifications.

- A web-based forms application was developed at UVa (along with multiple test CAs) that illustrates the use of the bridge architecture. Uses of the bridge that involved certificates from commercial CAs and the Virginia pilot CAs was also demonstrated.

Draft versions of the CP and CPS for the bridge are being developed.

APPENDIX I

DIGITAL SIGNATURES BUSINESS CASE

October 2000

INTRODUCTION

The traditional business case weighs tangible, quantifiable factors against the associated risks and costs to determine whether a given product or service provides value and is cost-justified. Does this technology increase worker productivity? Eliminate waste and redundancy? Streamline service delivery? Reduce costs? Foster substantial cost-savings? Based on the data, the leader can evaluate the potential impact and is equipped to make a technology decision.

The digital signatures decision is not strictly a technology decision—it is a business decision about technology. The traditional business case does not work for digital signatures because it encompasses more than a single product or service—it is a shift from the “business as usual” paradigm and fundamentally affects how government communicates with and serves its customers.

As seen in the demonstration effort, digital signatures provide benefits that are difficult to quantify. How much is “trust” worth? How do you quantify the value of non-repudiation support? The value of modifying or removing archaic business processes? How much does it “cost” if confidential data—such as medical records—is accidentally released to an unauthorized source? What dollar value can be placed on customer satisfaction?

GOVERNOR GILMORE’S VISION FOR ELECTRONIC GOVERNMENT

“The Digital Dominion” is Governor Gilmore’s vision for electronic government in the Commonwealth. The Governor built The Digital Dominion on the tenets of simplicity, flexibility, and consistency to ensure streamlined, effective delivery of government services and increase active participation among citizens, businesses, and employees in their government. Governor Gilmore’s vision for electronic government extends beyond hardware and software and web sites. The Commonwealth seeks to deliver electronic services across all levels of government and use technology to break down barriers that distance people from government services. In other words, the primary goal of electronic government in the Commonwealth is to improve government services delivery.

One of the barriers to interactive e-government is lack of trust. Highly publicized events, such as identity fraud and breaches in security resulting in the compromise of confidential information, disruption of services, and destruction of data and systems, have created worldwide concerns over security of conducting business online. According to experts, distrust is the primary reason why individuals choose not to conduct transactions online—when I cannot see you, how do I know you are who you say you are?

Digital signatures is one of the building blocks to establishing trust online. Recognizing the need for and value of electronic signatures in the Commonwealth, Governor Gilmore signed the Virginia Uniform Electronic Transactions Act (UETA) earlier this year, giving electronic and digital signatures legal stature in the Commonwealth. Shortly thereafter, President Clinton signed the Electronic Signatures in Global and National Commerce Act into law. To further agency and institution adoption of electronic and digital signatures, Governor Gilmore created Executive Order 65, which directs “Executive Branch agencies and institutions to take advantage of the benefits of digital signature technology to the fullest extent possible.”

BENEFITS OF DIGITAL SIGNATURES

Before these critical pieces of legislation were passed, transactions involving signatures could not be fully automated. Due to legal requirements for wet signatures, electronic documents needed to be produced in hard copy for signature and stored in paper files to establish an audit trail. The primary benefit of electronic signatures generally and digital signatures specifically is full automation of processes that require signatures.

Digital signatures are one form of electronic signing and one form of authentication. Other options—used singly or in combination—include double-clicks, passphrases and PINs, hardware tokens and smartcards, and biometrics. On the spectrum of electronic signatures, digital signatures are at the top. Digital signatures offer the highest level of assurance, and—unlike nearly every form of electronic signature—provides for authentication, data integrity, and non-repudiation support:

- *Authentication*. Digital signatures are tied to specific identities and can help prevent fraud. A digital signature allows the relying party to determine—at a high assurance level—that the signor is who he or she claims to be.

- *Integrity of data*. Using a hashing function, digital signature technology computes and compares message digests to ensure data was not altered prior to signature verification. Because paper records can be altered easily and with few clues as to when the unauthorized modifications took place, digital records can be an important tool for fraud prevention.

- *Non-repudiation.* Because digital signatures are tied to specific individuals and are a legally accepted form of signature, they are legally binding.

Digital signatures are not an either-or proposition—they are one tool for enabling secure transactions, and should exist in conjunction with other forms of security and electronic signatures. Similarly, digital signatures in and of themselves do not provide the basis for e-government. An absence of digital signature capability in the hierarchy of electronic signatures, however, can be an impediment to effective e-government.

ASSOCIATED PROCESS REENGINEERING

In his keynote address at the Commonwealth of Virginia Information Technology Symposium in September 2000, Microsoft Executive Robert MacDowell urged the Commonwealth to blow up bad processes—to destroy bad processes completely and replace them with streamlined, functional automated systems that make good business sense. Web- or PKI-enabling an application can involve a great deal of up-front investment in dollars and time. There is little to no value in moving a bad process to an electronic environment—little or no value in using scarce technology dollars to automate a flawed process.

The greatest potential value may derive from the process of reengineering workflow and applications to create a customer-oriented electronic environment. Customer transactions that currently take days to go through a manual process will be redesigned to allow real-time, interactive transactions that can be completed in minutes.

Digital signatures represent an opportunity to evaluate workflow and business processes, and shift to a more citizen-centric view. Clearly, citizen demands and expectations and Governor Gilmore's vision for electronic government require that the Commonwealth reengineer processes and fundamentally change the way services are delivered to meet the needs of employees, businesses, and citizens.

RAISING STANDARDS

Digital signatures and automation present opportunities to raise standards for business processes, workflow, and security, and improve and redefine best practices. We want to put a working philosophy in place that we not replicate the security and accountability weaknesses and vulnerabilities often inherent in paper-based processes as we transition these processes into the electronic world. Several pilot participants found, for example, that digital signature technology provides a stronger audit trail and added security in terms of data integrity and authentication. The DMV travel reimbursement pilot, for example, 'locked' travel expense data in the form once the traveler signed it, so that it could not be altered.

COST-SAVINGS BENEFITS

The DSI Demonstration projects provided evidence of the intangible benefits of digital signatures, such as customer satisfaction, increased security, and an environment of trust. The "intangibles" provided sufficient value to four pilot organizations to compel them to move the pilots to a production environment. That is not to say there are not tangible benefits to digital signatures. There are. In the demonstration pilot effort, for example:

- *Virginia Department of Transportation* realized savings by eliminating the extra step of keypunching requirements in the procurement process. As a result, the awards process can be expedited. Data entry in the manual process takes 24 to 48 hours, depending on the scope of the bid. In comparison, the automated system transfers the same information electronically in 20 to 40 minutes.
- The *Counties of Chesterfield and Fairfax* experienced three-week time-savings in the end-to-end Mobile Home Sales Tax and Additional Rental Sales Tax digital signatures pilots. Revenue was transferred in a more timely manner, allowing the recipients access to the funds more expeditiously and providing the opportunity to leverage increased interest rates.
- The *Department of Game and Inland Fisheries* experienced significant time-savings for field personnel in processing requests for purchases. DGIF employees are spread over the entire Commonwealth. With such a distributed network of employees, savings were realized in reduced handling of paper, postage, and data entry efforts, as well as physical record storage. Purchase requests filed electronically with digital signatures generally require one day for processing, whereas in the manual system, the turnaround time was three to five days.

AN ENTERPRISE SOLUTION

Agencies and institutions in the Commonwealth traditionally choose to create, operate, and maintain their own individual systems and technology solutions. Because digital signatures are most valuable for high-risk transactions where anything less than a digital signature would be unacceptable, most agencies and institutions would find it cost-prohibitive to develop their own PKIs and security solutions. The DSI Workgroup believes the Commonwealth should adopt an enterprise solution of trust—a solution that offers a wide array of digital signature and PKI products, provides flexibility and simplicity, and promotes interoperability. By providing an enterprise solution, agencies, institutions, and localities do not have to invest significant time and resources in developing internal digital signature expertise and security infrastructure. A standards-based enterprise solution promotes interoperability, while allowing agencies, institutions, and localities to customize and adapt the technology to meet their business needs. Similarly, by articulating those standards, entities that choose to develop their own infrastructures will know the criteria to aim for.

DIGITAL SIGNATURES DECISION MODEL

By Audit & Assurance Team
August 14, 2000

INTRODUCTION

As the Commonwealth of Virginia embarks on development of a trusted online environment in which transactions with and within government will be conducted, it is important that good business sense continues to drive decisions concerning what to automate and how. Digital signature technology promises to provide a more secure electronic transaction framework than we have in place today. Along with the benefits, however, will come new risks to replace old ones, as with most new technology. These risks along with transition costs must be acknowledged and factored into the decision-making process.

To assist Commonwealth of Virginia entities, i.e. state agencies, colleges and universities, and local government, in determining when the use of digital signatures is appropriate, a decision model has been developed and is described in this section. Users of this model are advised to keep the following in mind:

- Decisions about the use of digital signatures should be made as part of an overall reengineering effort. Little value will be gained from using digital signatures "to pave cow paths."
- A decision to automate a manual signature is not necessarily a decision to use digital signature. Other electronic signature types, e.g. ID and password/PIN, may be perfectly acceptable in certain situations.
- The intended use of the model is for transaction-by-transaction decision-making. The model should help identify potential digital signature applications. It does not, however, provide all the guidance an entity may need to determine, in the aggregate, that a public key infrastructure implementation is desirable and viable, nor does it help shape the specific form that implementation should take.

A description and graphic depiction of the decision model follow, as well as a discussion of some additional decisions that must be made once it is determined that digital signature use for a given transaction is appropriate.

DECISION MODEL DESCRIPTION

In evaluating whether or not to utilize digital signatures, the first question to be answered is whether or not a signature (of any type) is required. In many cases, signatures have been used to acknowledge “notification” about a transaction but are not really needed to “authorize” a transaction. It is possible that a signature may not be “required” even though it has been the standard practice to obtain one. One step in determining whether to implement digital signatures would be for organizations to re-evaluate their processes, question whether the process makes sense and then decide if signatures of any kind are truly needed. If a signature is not critical and necessary to the institution’s mission and/or business process, then the implementation of a digital signature is not warranted.

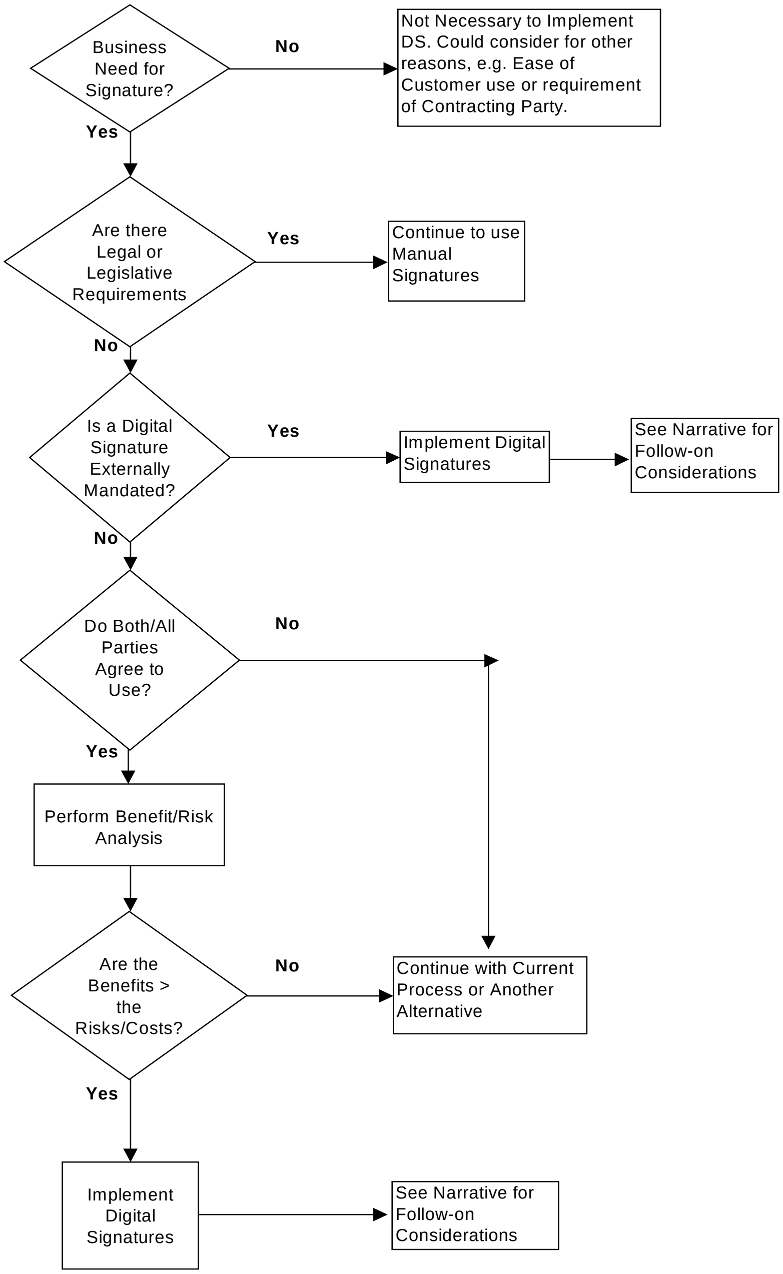
If it is determined that a signature is needed to “authorize” a transaction, the next question to be asked is whether a manual/”wet” signature is required by any sort of legislative body or law, e. g. the Uniform Electronic Transactions Act (UETA). There are some documents (wills, property transfers, divorces, etc.) that still require a manual/“wet” signature. If the transaction is one that requires a physical signature per UETA or other legislative authority, then digital signatures can**not** be implemented.

While there do not appear to be any instances that currently **require** a digital signature, there may be instances in the future where that will be the case. This is a likely scenario as the federal government moves to digital signature implementation. Under these conditions, an agency will have no alternative but to implement digital signatures.

If an agency determines that it does make “good business sense” to implement digital signatures, then both parties to the transaction must agree to the use of digital signatures. In many cases, especially with Government to Citizen transactions, there may be some reluctance to accept the use of a digital signature. In these situations, current processes could remain in place or alternatives would need to be arranged. This will require the parallel systems to be in place until all parties agree to use the digital signature.

The next question to be asked when determining whether to implement a digital signature is whether the quantifiable and non-quantifiable benefits to be derived will exceed both the costs to implement and the risks to be incurred. For example, if the volume of transactions does not support the implementation cost, then an institution may choose to continue using manual signatures. There also may be instances in which the agency makes a determination that a digital signature will not be used given the potential risks. If management determines that the benefits outweigh the identified risks and costs and the implementation supports the institution's mission, then digital signatures can be deployed.

DECISION MODEL GRAPHIC


Business Need for Signature?
No
Not Necessary to Implement DS. Could consider for other reasons, e.g. Ease of Customer use or requirement of Contracting Party.
Yes
Are there Legal or Legislative Requirements
Yes
Continue to use Manual Signatures
No
Is a Digital Signature Externally Mandated?
Yes
Implement Digital Signatures
See Narrative for Follow-on Considerations
No
Do Both/All Parties Agree to Use?
No
Yes
Perform Benefit/Risk Analysis
Are the Benefits > the Risks/Costs?
No
Continue with Current Process or Another Alternative
Yes
Implement Digital Signatures
See Narrative for Follow-on Considerations

FOLLOW-ON CONSIDERATIONS

Once a decision has been reached to use digital signatures in a particular transaction, there are further important questions that should be explored. These questions deal with document encryption, after-the-fact verification of signatures, long-term record retention, and private key security. These are briefly discussed below and further guidance is provided in the Audit and Control Standards section of this report.

Document Encryption. An online interactive session in which digital signing takes place could be encrypted using Internet security protocols, such as Secure Socket Layer. When the session ends, however, the digitally signed document(s) will not be stored in encrypted format unless the application explicitly allows encryption and the signer acts to encrypt the document(s).

Storage of encrypted documents requires that a complex key escrow mechanism be in place to ensure that those documents can be decrypted when users leave an organization, lose the private key, or otherwise cause the key to become unavailable. The decision to use document encryption is not a light one, since the technical and procedural implications are significant. Encryption should be considered for use only in cases where the document contains highly sensitive information and the negative ramifications of disclosing that information are significant for the organization.

After-the-fact verification of signatures. Because digitally signed documents replace hard copy, manually signed documents, new methods will be needed for verifying after-the-fact that a document has been signed by the person purported to have signed it. Once experience and court case history affirm trust in the technology to deliver on the promise of transaction non-repudiation, performing that verification may be as simple as confirming from an electronic log that a document was indeed signed on a given date and time by the person responsible for the private key. Until that time comes, however, further evidence, e.g. the complete electronic re-verification of the signature, may be desirable. Hence, when a decision is made to allow digital signatures for a particular transaction, a decision must also be made regarding the electronic information that must be stored with signed documents to allow after-the-fact verification.

As with document encryption, storage of this information requires that additional complex technical infrastructure and security safeguards be in place. Organizations should consider risk factors, such as transaction dollar value, in deciding how much information should be retained for a given transaction.

Long-term Record Retention. Converting manual documents to electronic form, either with digital signatures or without, does not in any way alter requirements to retain records for the entire retention periods as required by the *Code of Virginia* or Records Retention and Disposition Schedules. Meeting these obligations can be a challenge for electronic records, since a change in technology can render documents unrecoverable that are stored on older technology. It is important to understand that documents containing digital signatures cannot be reformatted, e.g. from a WordPerfect document to a Word document, in the normal way without losing the digital signature. The process of converting the document from one medium to another, e.g. from diskette to CD-ROM, however, will retain the digital signature.

A decision to move forward with manual to electronic conversion should, therefore, be accompanied by a decision on how converted documents will be stored, kept technically current, and eventually deleted at the end of their life cycle. It is advisable to include a verification of legal and legislative obligations as part of this decision process, as these may have changed.

Private Key Security. Without a secure means of protecting private keys from misuse, the business case for digital signatures is undermined. The association of a private key to an individual is critical to proving that a digitally signed document was completed by that person. The technology to authenticate an individual is maturing and good options are available in the marketplace. Any decision to use digital signatures in a given transaction should be followed by a selection of authentication options based upon requirements (dictated by level of risk), cost of available options, and implementation issues, such as ease of use and anticipated user acceptance. In medium to high-risk cases, the use of multiple options, such as the combination of a possession factor (e.g. smart card) and knowledge factor (e.g. password), may be prudent. The ANSI x9.49 standard referenced in the Control and Audit Standards section provides helpful guidance on this particular issue.

ELECTRONIC VOTER REGISTRATION AND ELECTRONIC VOTING

by Michie Longley, Department of Motor Vehicles

September 14, 2000

INTRODUCTION

Members of the Virginia Digital Signature Initiative (DSI) project believe that electronic voter registration and electronic voting can serve as a model for all other types of DSI applications. The e-voter issues are of such scope and extent that it would encompass all issues than must be considered. It will identify issues and obstacles that can be applied for other applications, thereby identify the issues and obstacles that would apply to any other application.

Internet Business — New communications and information technologies are revolutionizing the ways in which people communicate and conduct business. People can now communicate where and when it is most convenient, regardless of government and business hours of operations. More and more people today use electronic mail, the Internet and other such technology to communicate with each other and to conduct transactions with both government and businesses. Most private businesses and many governmental agencies have developed web sites to allow their customers to transact business 24 hours a day.

Equality of Access — At the same time, there is a growing acknowledgement of the so-called “digital divide” that separates those with access to this technology from those with no such access. Any discussion of electronic voter registration or electronic voting must take this division into account. Equality of access to the ballot box is a fundamental element of the democratic process, protected by federal and state laws. An electronic process for voter registration and voting should enhance the existing process so that all qualified voters have equal opportunity to exercise this right.

Security — Another issue has been illustrated by the recent hacker attacks on well-known web sites such as Yahoo and the Congress of the United States. The current paper-based system of voter registration and voting is protected and monitored to ensure the security and privacy of votes and records, and to investigate voter fraud and provide redress for any confirmed fraud. Any system envisioned for electronic voter registration or electronic voting must be private, accurate and secure from any interference. Network security and data encryption must be secure enough to ensure data integrity, and the electronic voter authentication process must be secure against possible fraud.

Policies and Systems — Finally, while technology can provide many benefits, it must be managed carefully. The existing framework of policies and systems that define and support the entire voter process must be reviewed and amended as needed. New policies and system supports will have to be developed to ensure that any electronic voter system supports the intent and legal structure of the voting process.

Any attempt to register voters or provide voting opportunities over the Internet must incorporate requirements in the following areas:

- ***Legal Requirements:*** State laws governing the electoral process will have to be amended. Federal laws relating to equal access and fairness in the voting process will have to be accommodated.
- ***Infrastructure and Process:*** The roles and responsibilities of all involved must be recognized, amended where necessary and possible, or accommodated and incorporated into the system design.
- ***Social Issues:*** Perceptions and concerns of election officials and the regulatory and legislative agencies involved in the election process and those of the general public must be considered when developing an electronic voting system. This is especially critical when a Constitutional right such as voting is concerned.
- ***Issues Relating to Voting and to Electronic Voting:*** Voter eligibility and identity are crucial concerns to election officials. Citizenship and residency are part of the determination of eligibility. In addition, certain applicants are deemed ineligible for felony convictions and court findings of mental incompetence. Finally, confirmation of identity, maintenance of ballot secrecy, and prevention of voting fraud are primary concerns at the polls.

- ***Technological Assumptions***: The system must provide a methodology to identify a voter while maintaining the secrecy of the voter and the vote. The system must be structured so as to ensure voter information is transmitted and maintained information securely and confidentially. A form of voter identification and identity verification must be built into the process, whether it involves issuance and use of a personal identification number (PIN), access or password code, digital certificates or a combination.
- ***Support for New System:*** Costs, equipment and training will be major prerequisites for the successful implementation of any new electronic voter registration or electronic voting system.

VOTING FRAMEWORK

LEGAL REQUIREMENTS

Federal and state statutes govern the current voting process. For any proposed DSI application, all relevant laws, regulations and statutes must be identified and accommodated where necessary. Specifications for the DSI application should include the provisions and conditions mandated by statute.

- **Federal Voting Rights Act (1965)** applies to states (mainly in the South) with a history of voter registration discrimination and denial of voting rights. This law places specific requirements on all phases of the voter registration process, including the location of polling places and hours of operation. Election officials must have any changes to the process, the applications and polling locations/hours approved ahead of time, or pre-cleared, with the US Department of Justice.

- **Federal Voting Rights Act for Language Minorities (1975)** applies to states and localities with a history of excluding citizens from the voting process by providing information in one language only. Non-English speaking citizens were deemed to be barred from the voting process through a number of practices and procedures in which information was communicated solely in English. This law mandates that information pertaining to the application and voting process, candidates, issues, and so on be provided in the specified languages as well as in English. Virginia does not come under the provisions of this law.

- **Federal National Voter Registration Act — Motor Voter Act (1993)** applies to all states and mandates that voter registration application occur simultaneously with a driver's license application or renewal. It also provides for voter registration applications in all offices providing public assistance. Because the voter application is considered an integral part of the driver's license process, driver licensing authorities in states whose electoral process come under the Voting Rights Act of 1965 now find that changes to driver's license applications must be pre-cleared by the Department of Justice. Electoral officials have had to make adjustments to their processes to accommodate the applications being received from the driver licensing and social services agencies.

- **Title 24.2 of the Code of Virginia** pertains to all aspects of elections (federal, state and local) and sets forth the various roles, responsibilities and requirements for elections officials. Sections are devoted to qualification and certification of candidates and elected officials, campaign finance reporting and monitoring, and qualification and application for voter registration. Section 24-2-411.1 specifies the process to be used to bring Virginia into compliance with the National Voter Registration Act. This Title also specifies the process, time frames and schedules for state, city, town and county regular and special elections.

INFRASTRUCTURE AND PROCESS

The federal government, state and local government, and the judiciary are all involved in the voter registration process. Roles and responsibilities of those involved are shown below.

FEDERAL ELECTION COMMISSION

- Controls and monitors all aspects of campaign finance – including funding and reporting criteria – and release of information.
- Enforces the provisions of the law such as the limits and prohibitions on contributions.
- Oversees the public funding of Presidential elections.
- Monitors states' compliance with voting laws.
- Sets national standards in equipment used to accept, record, and compile votes.

VIRGINIA STATE BOARD OF ELECTIONS

- Establishes and implements policies and procedures used to properly register voters and maintain voter registration records.
- Operates and administers a computerized central record-keeping system (the Virginia Voter Registration System) of all voters registered in the Commonwealth.
- Supervises and coordinates the work of local election officials.
- Provides printed ballots and computer generated lists of registered voters to each registrar for each election.
- Establishes regulations, issue instructions and other information to the local electoral boards and registrars to promote the proper execution of election laws.
- Qualifies or disqualifies candidates for nomination or election to federal, statewide, the General Assembly and shared constitutional offices.

US JUSTICE – CIVIL RIGHTS DIVISION – VOTING SECTION

- Reviews voting changes submitted to the Attorney General and makes recommendations for approval or disapproval.
- Brings suit to enforce, and defends suits in court relating to Section 5 (pre-clearance) litigation in court.
- Brings lawsuits against states, counties, cities, and other jurisdictions to remedy denials and abridgements of the right to vote.
- Reviews changes in voting laws and procedures proposed by states and localities for compliance with the provisions of the Voting Rights Act. Includes annexations and at-large election systems, redistricting, changes in polling locations and hours of operation, changes in voter registration process, etc.
- Monitors Election Day activities through the assignment of federal observers under Section 8 of the Voting Rights Act.

VIRGINIA CIRCIUT COURT JUDGES

By locality, the circuit court judges of that locality appoint the locality's Electoral Board.

- Appoints at least three citizens of the locality to the Board.
- Appoints members according to the two political parties with the highest and next highest number of votes in the last gubernatorial election.
- When possible, selects members from lists of nominees submitted by the political parties entitled to appointments.

VIRGINIA ELECTORAL BOARDS

- Appoints general registrar and officers of election for each precinct.
- Oversees preparation of ballots, and the administration of absentee ballot provisions.
- Oversees conduct of each election, and the ascertaining of the results of the election.
- Maintains records of the Board, open for public inspection.
- Administers election laws for the locality.
- Oversees general registrar's performance of assigned duties.

VIRGINIA GENERAL REGISTRARS

- Provides voter applications to the public and registration locations and registers voters.
- Maintains official voter registration records.
- Applies for pre-clearance approval from the US Department of Justice when voter applications, processes and polling changes are needed or when redistricting, annexation, etc., change political boundaries of precincts.
- Notifies applicant in writing when voter application is denied.
- Verifies the accuracy of voter lists provided by the State Board of Elections for each precinct.
- Reviews petitions to ensure those signing are registered voters of the locality.
- Send voter registration cancellation notices resulting from new voter registration to other localities within Virginia or other states as needed.
- Distributes and accounts for absentee ballots.

SOCIAL ISSUES

- **Access to Technology:** All U.S. citizens, with certain exceptions, [1] are entitled to vote. This right is guaranteed by the U.S. Constitution. Concerns have been raised that use of the Internet and other such electronic systems may have the effect of denying this right to those without the necessary computer literacy skills or lack of access to the necessary equipment. Studies show that minority groups overall and those in low income brackets have less electronic access and this has raised issues of equal access to the ballot box in the event of electronic elections.

  This issue has an additional significance in those states that are under the purview of the federal Voting Rights Acts. In those states, the voting forms and processes are used by state and local voting authorities are under continual review by the U.S. Department of Justice (DOJ) to ensure that fair and equal access to the voting process is maintained. Any changes to the forms or the voting process must be approved in advance by DOJ in a procedure called pre-clearance. The state or a locality within the state must submit a formal request to DOJ before any changes can be implemented. [2]
- **Safety and Secrecy of The Ballot:** Every locality is required to certify the results of any election. Part of that certification involves investigating any allegation of voter fraud. Voter fraud can encompass instances such as multiple votes cast by the same individual, fictitious identity, and undue influence on a legitimate voter.

  In addition, the current paper election process is designed to ensure that the choices made by each individual voter remain secret and anonymous. There is no information on the paper ballots now used that can identify the person who cast that ballot. An electronic voting system must ensure that the identity of the voter (provided through technology such as digital signatures or certificates) is separated from the choices made and cannot be reconnected.
- **Identity of Voters:** The prospective voter establishes identity at the time of voter registration. Ascertaining the identity of the voter at the polls is done in several ways: the voter can produce the voter registration

card received from elections officials, or provide a photo identification. Voters who registered by mail will be identified on the voter roll and will be required to provide this information. The information that is shown on these documents must match the information provided on the voter rolls in the polling location.

Once the voter is identified, the poll workers place a check mark by the voter's name on the roll. This ensures that if the voter engages in voting fraud and goes to another location to vote a second time, it can be identified and the voter can be prosecuted.

- **Personal Privacy:** Since electronic voting will involve a remote site that is not monitored or controlled by elections officials, they will be unable to verify the voter's identity prior to voting. Therefore, the electronic voter will likely have to be pre-registered with an electronic registration certificate and possibly a digital signature to ensure verification of identity prior to voting. On a national level there has been much discussion of and resistance to the idea of a national identity card. Resistance to use of social security numbers as an identifier is growing. It is possible therefore that the process for electronic voter registration will be seen as another threat to privacy.

  In addition, the current system requires voters to go to a precinct polling place to cast a ballot. This ensures that votes will be cast in private. Poll workers monitor activities to prevent any actual coercion or intimidation of voters. In a proposed remote voting location, there will be no guarantees of privacy or freedom from coercion.

TECHNOLOGICAL ASSUMPTIONS

Any system designed to provide electronic voter registration or electronic voting must be secure. In addition, it must provide foolproof voter authentication and proof of identity. It must prevent any release of information relating to the identity of the voter or the choices made by the voter.

The extent of the system will have to be defined and agreed to by those involved in the process. Once the basic system design is determined, the supporting practices and processes will have to be changed to match the new system. Training will be needed along with new or updated computer equipment.

Among the options that could be considered are using the Internet to provide:

- A supplement to the current absentee ballot process.
- An additional in-person vote recording system used in existing precinct locations.
- A system to collect and tally votes and relay the totals to elections officials.
- A central voting location controlled by election officials, but located in untraditional sites such as shopping malls.
- Remote sites such as the voter's home, where the voter accesses the voting web site to cast a ballot.

Depending on the extent of electronic support provided, system design should incorporate the following provisions as needed:

- **Identification and Registration of Voters:** As identity is a major issue in the voting process, any system proposing electronic voter registration should have a process to ensure the identity and registration of citizens before they cast a vote. A system to document and retrieve registration must be established as the first part of any electronic voter registration process. The system must also be able to verify that the prospective voter is a real person and is eligible to vote.
- **Authentication of Voters:** At the time of voting, the identity of the person wishing to vote must be authenticated. If the system envisions use of remote sites without oversight by elections officials, some component of identification verification will be needed. This can include technology such as biometric identifiers, encryption and digital signatures, smart cards, etc. The integrity of the voting process depends on each eligible voter casting a single ballot.
- **Security Against Fraud**: Any system used for electronic voting must be designed to prevent fraud. The possibility exists for hackers and others to amend or falsify voting information, or to create phony look-alike web sites which would divert the votes to a non-authorized location or delete the votes entirely.

- **Security of Transmitted Information:** The system must be designed to ensure that information related to the actual voter is rendered anonymous and irretrievable. It also must ensue that the vote is transmitted secretly and accurately.
- **Vote Delivery:** Any system used to collect, compile and deliver electronic votes must maintain the privacy and integrity of each ballot cast.

PREREQUISITES TO IMPLEMENTATION

DESIGN THE NON-AUTOMATED PROCESS FIRST

Elections officials, registrars and members of local Electoral Boards should work together to define the non-automated process that would be necessary to support an Internet voter registration/voting system.

The electoral process is controlled mostly from the local level, although all parties involved must approve and support any new system. All those involved must approve any new system – this is not a case where some localities can implement a new process. The system must be designed for statewide, universal implementation. In states under the purview of the federal Voting Rights Acts, the U.S. Department of Justice must approve any proposed changes before implementation.

- **Determine options for how will the technology be used.** Will this option apply to only the registration of voter applicants? Will the technology involve using form downloads or will it enable full automation to accept application information online? Will the system be designed as a supplement to the current absentee ballot process? Will it serve as an additional in-person vote recording system used in existing precinct polling locations?

Will it be installed to collect and tally votes and relay the totals to elections officials? Will it be placed in non-traditional voting locations controlled by election officials (or not) located in sites such as shopping malls? Will it be designed to accommodate remote sites such as the voter's home, where the voter accesses the voting web site to cast a ballot?

- **Determine and analyze the implications of the above to help define the new process.** What impact will the use of PC's in remote locations have on the current location-based process (i.e., where applications have to be processed and stored by the registrar of the applicant's resident locality, and where voters are assigned to a brick and mortar polling site)? Will voters need a form of automated identification and/or authentication such as a digital certificate? How will this identification be authorized and issued, and by whom? Will it tie into a statewide system? How much security is needed in the processing and handling of voter applications? Of ballots? What changes will have to be made to the current process?
- **Determine what laws will need to be written or changed to enable this process.** Determine whether any changes to state laws will be needed. If enabling legislation is needed, are there parts of an Internet system that can be implemented without statutory changes? The US Department of Justice must approve all changes (to process, automated systems, forms) before anything can be implemented.
- **Determine what policies, regulations and procedures will have to be written or changed.**
- **Assess current proposals to develop the architecture for statewide electronic signatures.** Are there any needs that will not be met by a statewide architecture? How critical are they? Assess levels of security and authentication. Will they meet those needed for the electronic voter registration process or electronic voting? Assess levels of automation and technology that will be needed to support this architecture. How will we be able to acquire, install and support it statewide?

DESIGN THE AUTOMATED SYSTEM TO MATCH AND SUPPORT THE PROCESS.

- **Identification and Registration of Voters:** As identity is a major issue in the voting process, any system proposing electronic voter registration should have a process to ensure the identity and registration of citizens before they cast a vote. A system to document and retrieve registration must be established as the first part of any electronic voter registration process. The system must also be able to verify that the prospective voter is a real person and is eligible to vote.

- **Authentication of Voters:** At the time of voting, the identity of the person wishing to vote must be authenticated. If the system envisions use of remote sites without oversight by elections officials, some component of identification verification will be needed. This can include technology such as biometric identifiers, encryption and digital signatures, smart cards, etc.
- **Security Against Fraud**: Any system used for electronic voting must be designed to prevent fraud. The possibility exists for hackers and others to amend or falsify voting information, or to create phony look-alike web sites that would divert the votes to a non-authorized location or delete the votes entirely.
- **Security of Transmitted Information:** The system must be designed to ensure that information related to the actual voter is rendered anonymous and irretrievable. It also must ensue that the vote is transmitted secretly and accurately.

DEVELOP NEEDS FOR EQUIPMENT, TRAINING AND ASSOCIATED COSTS.

- What costs will be involved? If additional funding is needed, how will it be procured? What new equipment will be needed? In what time frame? How will it be acquired?
- What training will be required to implement this new process for current employees? Will new employees be needed to support this system? How long will it take to hire and train new employees and train existing employees? Will each agency conduct the training or hire someone to do it? How will training be funded?

CURRENT INITIATIVES

The federal government, several states and some localities have initiatives underway that would allow electronic voting or propose to study the issue. They include:

ALASKA: The Republican Party of Alaska held its first straw poll prior to the January state presidential primary. Thirty-five voters in three remote northern districts (Districts 36, 37, and 38) were able to participate through the Internet. [3] There were no reported problems with use of the Internet.

ARIZONA: The Arizona Democratic Party conducted its May 2000, presidential primary through the Internet as well as by traditional methods. The results were a total turnout of 86,907 voters, an increase over the 12,800 voters who participated in 1996.

- 35,768 voters cast their votes through the Internet from remote locations
- 32,748 voters mailed in their ballots
- 4,174 voters used the Internet at their polling locations
- 14,217 voters used traditional paper ballots at their polling locations. [4]

The plan to allow online voting was opposed by the Virginia-based Voting Integrity Project, who sued to stop the electronic process based on discrimination against poor and minority voters. A federal appeals court judge dismissed the suit, and the electronic process was further approved by the Department of Justice. While no fraud has been reported to date, voters did report difficulties in getting online and busy telephone help lines.

CALIFORNIA: The California Internet Voting Task Force recently released its findings. The task force was formed in April 1999, and its members included government and elections officials as well as voting advocates and technical staff. While the task force recognizes that it is possible to use the Internet for voting, it recommends a go-slow approach. It favors using the Internet as another form of voting to supplement and augment the traditional methods, and believes it should be phased in over several years.[5]

WASHINGTON: Thurston County voters cast votes via the Internet during a non-binding, mock election held on February 29, 2000. It was held in conjunction with state presidential primary. Over 3,000 voters used the Internet, and over 90 % stated that they would use the Internet again if it is offered as a voting option. [6]

FEDERAL GOVERNMENT:

- The Digital Democracy Study Act of 1999 [7] was introduced and referred to the House Committee on House Administration on 11/5/99. This bill would direct the President to study and report to Congress on issues raised by the incorporation of online and Internet technologies in the voting process.
- The Congressional Internet Caucus Advisory Committee was established in 1996. It has 166 members from both sides of the Congress, and its purpose is to educate Congress on the potential of the Internet. It recently published a call for volunteers to serve on a panel studying issues and obstacles to online elections. [8]
- The Department of Defense (DoD) will offer the option of Internet voting in the 2000 presidential election to member of the U.S. armed services. This pilot program is a cooperative effort between DoD and the following localities:
- Oskaloosa and Orange Counties, Florida
- Buchanan and Jackson Counties, Missouri
- Dallas County, Texas
- Weber County, Utah
- Any county in South Carolina.

Service members who wish to use the Internet to cast their votes must volunteer for this program, be legally registered to vote in one of those localities, must have applied to cast an absentee ballot, and must have access to the Internet. Software will be provided to these volunteers, and votes will be cast through access to the Pentagon's public key infrastructure. After the election, DoD and the states will analyze the results with a specific emphasis on the integrity of the process, ease of use, response time and overall system security. [9]

RECOMMENDATIONS

Given the complexity of the topic and the numerous legal, social and technical issues involved, a slow and cautious approach is essential. Security and accuracy are paramount concerns that must be ensured in any system design. Use of digital certificates can raise the security level, but there must first be an operational, reliable process that certifies and registers identity and issues the certificates. At this time, digital certificates are not in wide use. In addition, election laws will have to be reviewed and revised before any substantial use of electronic voting can be implemented.

Until such a method has been established, a first step to electronic voting could be considered. Installation of an electronic system in current polling locations and under the control of elections officials could be considered. Citizens could use the Internet connection at that location to cast their ballots, but would still be required to verify their identity to an elections official. However, security and privacy will have to be guaranteed before any expansion of e-voting systems.

[1] Those with felony convictions and those adjudicated mentally incompetent are denied the right to vote unless their voting rights are restored (usually by the courts or the Governor, or by petition to the President for federal crimes).

[2] The preclearance process is mandated by the Voting Rights Act of 1965 (42 U.S.C. 1973 et seq.) and controlled by regulations contained in the Code of Federal Regulations, 28 CFR Ch. 1, Part 51.

[3] Source: Republican Party of Alaska web page http://www.alaskarepublicans.com/straw.htm

[4] Source: Arizona Democrats web page http://www.azdem.org/breakdown

[5] Source: California Internet Voting Task Force: A Report on the Feasibility of Internet Voting, January 2000. Available at http://www.ss.ca.gov/executive/ivote

[6] Source: Thurston County, Washington, Auditor's web site: http://www.co.thurston.wa.us/auditor1/index.htm. Auditor's evaluation and report is available at this site.

[7] Source: U.S. Congress on the Internet site: http://thomas.loc.gov/

[8] Source: U.S. Congressional Internet Caucus web site: http://www.netcaucus.org/events/evoting2000.shtml

[9] Source: Department of Defense, American Forces Information Service news article, September 13, 1999. Web site for article: www.defenselink.mil/news/Sep1999/n09131999_9909133.html

APPENDIX L

EXECUTIVE ORDER 51 REVIEW

August 30, 2000

INTRODUCTION

In December 1998, the Governor's Commission on Information Technology issued a series of recommendations, contained in its report "Toward A Comprehensive Internet Policy for the Commonwealth of Virginia," related to the expanding use of the Internet and electronic commerce in Virginia. The 1999 General Assembly enacted several pieces of legislation that, taken together, embody the Commission's recommendations for a Virginia Internet Policy Act.

In addition, the Commission made a number of recommendations specific to state government agencies and institutions that can be implemented administratively. These recommendations recognize that the Internet is a tremendous tool for effectively and efficiently delivering government services to the citizens and businesses of the Commonwealth. These recommendations also recognize that access to the Internet is essential to full participation in the modern economy. No sector of the Commonwealth's citizens should be left without access to this important resource.

As one of ten specific policies listed under Executive Order 51, the following directive was given which may have application to the Digital Signature Initiative in the Commonwealth:

A. All Executive Branch agencies and institutions shall develop plans for delivering current and expanded services through the Internet and shall submit these plans to the Department of Technology Planning (DTP) for review no later than June 1, 2000. Such plans shall maximize workstation access to Web-based transactions by agency and institution employees for use in their work assignments and in their status as state employees. In developing such plans, agencies and institutions are encouraged to consider partnering, where appropriate, with the Virginia Information Providers Network Authority (VIPNet) to deliver such services. The VIPNet Authority Board of Directors will review the partnership opportunities, issues and needs expressed in these plans for potential inclusion in its annual business plan.

To complete this directive, the following instructions were provided to all applicable agencies and institutions:

1. Use **Business Applications** that are most meaningful to your agency or institution. The level of detail should be sufficient to indicate the specific services provided to external customers (citizens, companies, or other organizations, other governmental units, etc.) and/or the business interactions the agency has with those entities. Internal applications may be listed but are not required.

2. Indicate the total number of **currently existing forms** that are included in the application.

3. Each Business Application should be associated with one or more **Priority Business Activities**. These are the Functional Activities, ranked in priority order, that the agency defined as part of the Department of Planning and Budget's Performance Budgeting Process.

4. Report Web enablement plans by the **Tiers** defined in *Agency/Institution Web-Site Planning Guide & Plan Template* distributed for the February 18 Executive Order 51 Workshop:

   - Tier One—No forms on Web-site
   - Tier Two—MS Word (or other off-the-shelf software used for forms)
   - Tier Three—PDF formats for forms
   - Tier Four—HTML (interactive) formats for forms
   - Tier Five—HTML formats with digital/electronic signature

Tier Two is the minimum required for forms to meet the December 31, 2000 Web-enablement requirement in the Governor's Executive Order 51.

EXECUTIVE ORDER 51 REVIEW

The following review was conducted with an eye to identifying additional areas that may need to be addressed in the report to COTS. It was also conducted with the intention of providing guidance to agencies that intend on implementing the use of Tier 5 forms (using electronic or digital signatures) with external parties. Special attention was paid to an organization's technology infrastructure, customer base, and number of annual transactions (if listed).

Entities that did not list the need for Tier 5 forms or provide mention of electronic signatures, digital signatures, or PKI are not listed. Unless specifically noted in the agency documentation, Tier 5 cannot be determined to be either digital signature or electronic signature. If a narrative in support of their forms' plan was not available, no commentary was provided.

It is quite clear that many entities need (and plan) to perform a reengineering of their forms to determine revisions and possible elimination of some forms altogether. Since this reengineering task was not performed prior to submission of their EO51 documentation, perhaps many forms listed for use with electronic signatures will, in fact, be eliminated, or determined not to require a signature.

Based on the above comments, several recommendations have come out of this review as follows.

1. Distribution of COTS Digital Signature Initiative final report to all agency heads and authors of the EO51 documentation to supplement their planning efforts.

2. An Education program targeted at all entities considering implementation of Tier 5 forms. This program would include PKI and digital signature basics (what it is and what it is not), the importance of reengineering as it relates to forms, the process to follow in reengineering forms (proposed decision model), entity infrastructure required, and consideration of Digital Divide issues.

   The purpose of this program would be to solidify a base of realistic participants now and in the future.

EXECUTIVE ORDER 51 REVIEW

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Charitable Gaming Commission			A number of forms are available to the public such as licensing application, bingo supplier application and forms required for altering one's license. The future of interactivity with these and other forms will depend on the ability to implement electronic signature and to collect fees electronically with the submittal of applications and reports.
Compensation Board	1 1	2002 2003	Local Inmate Data System and State network Interface Project forms. The Board's budget requests for appropriate resources to accomplish these tasks were not approved in the upcoming biennial budget. It is unlikely the agency will be able to become fully web-accessible to our constituents within the time frames listed by relying solely on current staff and limited funds budgeted for minor system enhancements.
Elections, State Board of	1 2 4	2002 2003 2004	Due to the criminal nature of voter fraud activity, and the reluctance of the Commonwealth's Attorney to prosecute such cares without a perfect case, it is expected that original signatures may continue to be recurred by the General Assembly for several years on certain documents (such as voter registration applications) until case law is further developed involving digital and digitized signatures.
General Services, Department of			A significant number of Web interactive forms will be located on the new COVA e-procurement portal. They will consist of forms currently available on the existing Division of Purchasing and Supply's web site and new forms to be developed by the contractor. These forms to be developed will include fully interactive vendor registration forms, order forms, e-mall forms and standard model RFP/IFB forms and other purchasing vehicles. These forms will include digital signatures or other security features necessary for secured bidding and purchasing activities. The COVA e-procurement portal forms will be at a minimum of Tier 4 with a target of Tier 5 based on the establishment of a functional PKI infrastructure including a COVA Certificate Authority and Registration Authorities accessible to the cities, counties, towns and suppliers of the Commonwealth. The Division of Consolidated laboratory Services (DCLS) involves the largest effort in posting forms to the Web. Due to the critical need for security of the data handled by DCLS the effort to upgrade to Tier4 and 5 will require digital signatures and encryption technologies now being evaluated by the Commonwealth. For this reason the Agency schedule shows the DCLS upgrades at the end of the project period. It is the hope that this can be accelerated as technology becomes available both to DCLS and its customers. A primary requirement is a PKI CA and RA accessible by the public health community in Virginia.
Human Resources Management, Department of	2 2	2001 (Jul – Dec) 2002	Includes Facility Reservation, Benefits Enrollment/Waiver, Recruitment, and Donations (Commonwealth of VA Campaign).
Human Rights, Council on	2	2002 (tentative)	The Council will consider Tier 5 applications to the complaint process (currently Tier 3), as well as documents provided to members across the state.

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Veterans Affairs, Department of			Legislation will determine whether or not forms will be provided with digital signature capabilities. Forms are derived from Federal government.
Economic Development Partnership, Virginia	29	2002	Priority business activities are: International Business Development and National Business Development.
Forestry, Department of	12	2003	
Housing & Community Development, Department of	20 43	2002 2003	These Tier 5 forms may be pursued, as state policies relating to such transactions become more defined. No immediate plans for implementation. Primary focus is low and moderate-income individuals and households, elderly and disabled citizens, persons and families that are homeless or in imminent threat of becoming homeless, and economically distressed or stagnant communities. Also served are partners that include professional organizations, nonprofit organizations, federal, state, regional, and local governmental agencies, and a variety of for profit corporate and business entities that are involved in community development and redevelopment enterprises. One of the critical areas in developing online information gathering and transaction processing at DHCD is the need to receive authentic signatures that are required for legal documentation of applications for financial and technical services. There is very little flexibility in eliminating these requirements.
Labor and Industry, Department of	11	2004	Total 59,400 annual transactions. Security will be upgraded as necessary to correspond with available transaction types. Agency privacy and security policies will be developed and posted. Responds to the concerns of 170,000 employers as well as local and community groups, organized labor entities, and the general public.
Mines, Minerals, and Energy, Department of	3 2 3	2002 2003 2004	Includes permitting, grants and contract awards, contractor registrations, and electronic bidding. Currently working on an electronic permitting project, which will allow customers to submit applications to conduct coal mining.
Minority Business Enterprise, Department of	4	2001 (Jul – Dec)	Includes Certification and D-CAF programs.
Professional & Occupational Regulation, Department of	21	2004	Includes Board applications and licensure forms. The Agency plans to accept applications for licensure at the Tier 5 level for those professions and occupations where statutory and regulatory requirements allow. The regulatory boards license or certify more than 240,000 regulants.

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Arts, Virginia Commission for the	1	2004	The planned Tier 5 form is for a Technical Assistance grant, which has approximately 250 transactions annually. Other grant applications incur 16,920 annual transactions.
Christopher Newport University	66	2004	
Deaf & Blind & Multi-Disabled at Hampton, Virginia School for the			Projected plans for FY2002 and 2003 include providing the capability to attach signatures to applicable forms. The agency will continue to evaluate its current and future needs concerning form accessibility and relative security issues.
Deaf and the Blind – Staunton, Virginia School for the			Projected plans for FY2002 and 2003 include providing the capability to attach signatures to applicable forms. The agency will continue to evaluate its current and future needs concerning form accessibility and relative security issues.
Education, Department of	1 3 2	2002 2003 2004	
George Mason University	1	Current	Financial Aid Application (PIN authorization). GMU has interpreted Tier 5 as a category defined by law, i.e. there is either a state or federal regulation that requires the signature be authenticated. For example, the application for admissions from has a signature line on the paper version. The Web version does not because there is no law requiring a signature. On the other hand, some of the university's Tier 4 forms do allow for credit card payments through a secure server. These forms have not been classified as Tier 5 because there is no law requiring an authenticated signature.
James Madison University	1 3	2002 2003	Includes Computing, Student Records, Employment and Procurement.
Jamestown-Yorktown Foundation			In FY2001 the agency will explore partnership possibilities to offer online ticketing. Implementation of online ticketing will depend on financial resources. This technology would need to be Tier 5 at implementation.
Library of VA	8	2004	(includes) Certificate of Records Destruction, Records Transfer List and Receipt, Interlibrary Loan Patron Request form, Application for a Library Card. Annual transactions = 15,060. Some forms requiring multiple signatures, third-party signatures, initials, or notarization are not scheduled beyond Tier 3. The agency will re-evaluate these and other forms as the availability, acceptance and adoption of digital signatures grows and the technology, standards and capabilities evolve.

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Marine Science, Virginia Institute of	1 3	Current 2003	Includes graduate program application and online course materials. Online course materials include interactive testing, online discussion, reserved readings, grading and evaluation components.
Mary Washington College	12	2002	Includes applications for admissions, licensure, tuition, and course registration. Jan – June 2001: Begin adding digital signature capability to specific forms, following the guidelines developed by DTP. Research for electronic business partners. Convert intra-agency Tier 4 forms requiring a signature to Tier 5 level.
Old Dominion University			A review of possible Tier 5 forms will be conducted after 12/00. The move to these types of forms and the timing of such moves are dependent on current Commonwealth initiatives regarding digital signature, possible changes in laws or policies, and whether security concerns can be properly addressed.
Radford University	4	2003	
Science Museum of Virginia			The agency is developing e-commerce capability for ticketing and other transactions with the public.
University of Virginia			PKI will serve as a central security element in the University's new integrated system scheduled to come into production in phases over the next five years. It is too early to identify the specific forms or processes, some of which may not exist at this point in time, that will be impacted.
University of Virginia's College at Wise			Support for interactive forms and digital signature requirements will be a team effort and coordinated with the university's Integrated Systems Project.
Virginia Commonwealth University			VCU has begun the process of planning for the replacement of all major administrative computing systems. VCU prefers to replace the current systems with an integrated set of applications sharing a common database with Web access an inherent part of their design. Enterprise Resource Planning systems will provide such capabilities and provide such features as: Use of authentication and digital signatures to ensure a proper level of security and privacy for processes and information. VCU's ultimate goal is to convert all forms required by the University' schools and departments to the Internet. VCU will evaluate the purpose of each form, ascertain its business purpose, and formulate a plan for converting to a direct update process via the Internet. The Criteria for evaluation will include…acceptance of digital signatures, … Implementation of an ERP-like system is planned to occur within a six-year timeframe.
Virginia Community College System	1	Not specified	

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Virginia Polytechnic Institute & State University			VA Tech will investigate moving some forms to Tier 5 once they have determined the appropriate PKI infrastructure to implement.
William and Mary, The College of			The College is currently in the process of developing an integrated administrative information system that will allow online processing and completion of most transactions required by both internal and external customers through the web. Once the detailed plan is complete, a comprehensive web strategy supporting the plan will be developed which will provide the infrastructure to support technologies such as digital signatures and certificates, secure servers, encryption and other security.
Accounts, Department of			
Planning & Budget, Department of			During the first half of FY2001, DPB is planning to evaluate the possibility of creating several interactive activities that could be utilized by state agencies during the budget development and legislative review processes.
Taxation, Department of	15	2001 (Jan – Jun)	
Treasury, Department of the	16	2004	The most frequently used form by citizenry at the Dept of Treasury is the Unclaimed Property Claim form. This form is currently on the web in HTML format, however, because of the legal implications of claiming property – proof of identity is required as well as any supporting documents by a claiming legal heir – this form cannot currently be made interactive. However, with the proliferation of digital signatures the form will eventually be available in the Tier 5 format by the end of FY2004. It is important to note, however, that while state agencies and businesses will take the lead in the popularizing of the digital signature, the public may lag significantly behind in adapting to and implementing the new technology.
HEALTH AND HUMAN RESOURCES			
Comprehensive Services for At-Risk Youth & Families	1	2001 (Jan-Jun)	Pool Reimbursement Request
Health Professions, Department of	82	2002	Licensure Applications: 19,836 yearly transactions Acceptance of checks and credit cards over the internet begins in Fall 2000 The agency wants to participate in Tier Five formats with digital/electronic signatures, but realizes that there is additional work that needs to be done on both COVA and agency's legislative/policy side. Some re-engineering of agency Board policies and practices will need to take place to overcome current practice of requiring notarized applications, thumbprints, imprints of state and school seals, multiple level signatures, and the acceptance of only checks or money orders.

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Health, Department of	3 8 1	2002 2003 2004	
Medical Assistance Services, Department of	150	2002	Recovery of Medicaid Services: States must try to recover costs of Medicaid services by (1) imposing liens on property sold by Medicaid patients and (2) seeking recovery from the estates of nursing facility or medical facility patients who were 55 or older when they received Medicaid services. Implementation of digital signatures would assist in meeting constituent expectations in the following areas: timely receipt of a health benefit (program beneficiaries), accurate and timely payment for services rendered (health care providers), maintenance of program integrity through detection and elimination of fraud, waste and abuse (taxpayers), and administration of the Medicaid program within federal laws and regulations (Health Care Financing Administration) Once digital signatures and electronic forms become available a significant investment in computing hardware will be necessary. Staff resources may also become strained, supporting 24x7 coverage of a new web site. By FY2003, interactive cost reports will carry digital signatures allowing the provider community to submit electronic cost reports. These migrations will decrease the time spent sending and reviewing cost reports and determining reimbursement rates, while enhancing communication with the provider community in a secure Internet environment. One of the core business applications is healthcare claims processing. The 35 forms that are used support the ability to seek partial or full reimbursement for services rendered under state and federal regulations. Since these forms and applications could involve sensitive healthcare data security and privacy are primary considerations. In addition, these forms often require signatures and, therefore, can only migrate to a full Internet environment when digital signatures are employed, currently targeted for FY02. Most eligibility forms carry identifiable individual information including social security number, medical data, and require signatures. For that reason, these forms will not become interactive until the digital signatures are available with high-level security. The federal Health Insurance Portability and Accessibility Act (HIPAA) security standards, privacy policy and procedures, employer identifiers and provider identifiers will be determined over the next 26 – 38 months.

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Mental Health, Mental Retardation & Substance Abuse Services, Department of	4	2002	Includes licensure applications Exploring secured technologies and secured areas on web site for storage of sensitive information not available for public viewing. Many forms do not require a signature and are purely informational. Some forms require a “wet” signature. Some legal forms require signatures of a judge or magistrate. Criminal history checks require two signatures (which are required by law for employment at a private placement).
People with Disabilities, Virginia Board for	9	2002	includes Grants Management Establishing web-hosting services for the internet and intranet to provide better control, security and backup by 06/31/00.
Rehabilitative Services, Department of	49 2 20	2002 2003 2004	Establishing web-hosting services for the internet and intranet to provide better control, security and backup by 06/31/00.
Social Services, Department of	22	2004	Application for assistance, report changes, and appeal forms in the following areas: TANF, Food Stamps, Medicaid, Auxiliary Grants, General Relief, Energy Assistance.
Visually Handicapped, Department for the	2 41 52	2002 2003 2004	Includes Petty Cash Reimbursement and Request for Travel Authorization Establishing web-hosting services for the internet and intranet to provide better control, security and backup by 06/31/00.
Environmental Quality, Department of	24 8	2002 2003	DEQ form for information submission, application and registration require signatures. The current VA electronic signature law opens many doors to the agency. A majority of programs are conducted under delegation from the US Environmental Protection Agency. DEQ is currently working with USEPA on two pilot projects to be completed by the end of FY2001. These include Permit Applications and Discharge Monitoring reports. The current network infrastructure of the agency will not support Tier 4 and 5 forms. Additional hardware and software will need to be purchased over the next two biennium. Most Tier 5 forms will be postponed until 2002 to determine the USEPA’s electronic signature requirements.
Game & Inland Fisheries, Department of			The agency will be continuing its efforts to develop an electronic point-of-sale licensing system to facilitate and streamline the issuance, reporting, and accounting of hunting and fishing licenses. The Department is also working with other entities to develop online interactive (Tier 4/5) renewal of boat registrations. Some regulatory changes may be required to allow for electronic signatures in those cases where a signature is currently required. Given the time required to effect proper regulatory changes, they do not anticipate completing these earlier than FY03. In FY04, DGIF will implement digital signatures for those few remaining forms (primarily Boating) where required and appropriate.

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Museum of Natural History, Virginia			VMNH will add electronic signature recognition capabilities to its web offerings by the end of FY2002.
Criminal Justice Services, Department of	16	2002	Includes grants administration forms. At any point in time there are 900 grants in force.
Emergency Management, Department of	1	2001 (Jan – Jun)	Local Situation report.
Fire Programs, Department of	1	2001 (Jan – Jun)	Ordering of training materials.
Juvenile Justice, Department of	15	2004	Expenditure reports, grant and research applications, health assessments, reimbursement requests, construction approval and incident reporting.
Military Affairs, Department of	4	2003	Limited interaction with citizens of VA. Mainly support missions assigned from Federal government.
State Police, Department of			Several forms available to the public must be notarized, and will continue to be available in PDF format. For several other public forms, the Dept requires authentication and original signatures. Once the finding of the COTS study on electronic signatures has been pilot tested, approved, and adopted, the Dept will make a determination whether these forms can be upgraded to Tier 5.
DIT	62	2001 (Jul – Dec)	DIT will review its inventory of forms and evaluate the contents of each against the current information requirement for the business process each supports. This analysis will most likely highlight opportunities for the consolidation and restructuring of many input forms as well as the redesign of underlying processes. Additionally, the implementation of the automated help desk may eliminate the necessity for several currently existing forms. Incorporation of electronic signature capability for select forms will be consistent with the implementation instructions of the Secretary of Technology.
Innovative Technology, Center for	5 9 5	2002 2003 2004	CIT, as a technology and knowledge-based organization working to solve problems for technology businesses, is interested in utilizing electronic services to maximize the efficiency of its workforce and to simplify the interactions with its customer base. CIT has adopted FormFlow software to enable staff to attach digital signatures for internal use. CIT is preparing to launch an online awards application process requiring the submission of a title page with original signatures while pursuing the adoption of a digital signature solution for the public.
Motor Vehicle Dealer Board	6	2000 (Jul – Dec)	Dealers will use their assigned PINs, which act as their moniker/signature, to identify themselves to gain access into the interactive system. The dealer number in conjunction with an ever-changing numerical passcode will be used as the unique customer identifier. This will be used in lieu of a digital/electronic signature.

ENTITY	TIER 5 FORMS	PROJECTED IMPL. DATE	ENTITY COMMENTARY
Motor Vehicles, Department of	1	2003	Application for Dealer/Drive-away/Office trailers plates: 6,250 annual transactions. DMV will not be able to move most forms to Tier (4) and 5 without imaging technology, a document management tool including an automated workflow process and a massive forms redesign initiative which will support interactivity with DMV's core systems.
Rail & Public Transportation, Department of	2	2002	Grant applications.
Transportation, Department of	3 1 4 4	2001 (Jan – Jun) 2002 2003 2004	

VOLT OPEN STANDARDS PROPOSAL

By Chip German, University of Virginia
August 28, 2000

One of the core concepts of the recommendations of the Digital Signatures Initiative Workgroup is that the Commonwealth can help guarantee a successful implementation of a PKI environment when some of PKI's potential complexity is reduced by strategic choices. The first choice we must consider is whether or not the Commonwealth will select a single, vendor-specific PKI technology to bring the simplicity that we need. This choice is not feasible, in our view. PKIs using various vendor technologies are already in place in some Virginia governmental entities, and business relationships with other governments (federal, state, and local) and non-governmental entities will show that a single vendor-specific technology is neither practical nor realistic.

Once we have ruled out a single vendor-specific PKI solution for the whole state, what is the next best strategy to limit complexity? The answer is not obvious, in part because much of the important discourse on this subject is affected by vendors who, quite naturally, lose motivation to participate when the notion that a single vendor-specific PKI solution is eliminated. However, there is an excellent strategy that is elegantly simple and that eases planning, implementation, management and review. This is the strategy of open standards – vendor-neutral standards whose purpose is to enable and promote interoperability.

By adopting a suite of open standards as the default recommended for governmental entities using PKI and digital signatures, the Commonwealth will ease the burdens of decision-making for all Virginia governmental entities implementing PKI, while giving them the flexibility to tailor their implementations to meet their individual business requirements.

We recommend that the Commonwealth establish the Virginia On-Line Transaction (VOLT) open standards to include, among others, standards for:

- Digital certificate structure, (X.509, version 3)
- Type of information to include in VOLT certificates (identity only, authorization to be handled by applications)
- Types of certificates issued (certificates for individuals at a high-assurance level with correspondingly stringent identification verification; certificates for business representatives also at a high assurance level; certificates for relying parties limited to Virginia governmental entities)
- Registration processes (specific to each type of certificate)
- Various operations related to certificate issuance and management (including CRLs)
- Retention of documentation related to on-line transactions

These components will be organized into policy and practice documents, some of which will be associated with object identifiers (OIDs) that would be listed in any certificate issued in conformance with the VOLT open standards.

We also recommend that the VOLT open standards environment include a VOLT cross-certification bridge (the prototype of which was tested by the workgroup in its demonstration projects) as one of the means through which the PKIs of governmental entities that issue certificates in conformance with the VOLT standards can expand their domains of trust.

Because of the need for flexibility, the Commonwealth will be wise to designate the VOLT open standards as recommended but not mandatory. Our experience in the workgroup indicates that, because PKIs can be dauntingly complex, governmental entities will be happy to use the simplified VOLT open standards whether they are operating and directly managing their own PKI or contracting for services from the Commonwealth's central PKI services vendor. The VOLT open standards mean that a governmental entity can take comfort that it is not making shortsighted technology and policy choices.

The VOLT open standards also provide a means by which persons responsible for applications that they wish to use digital certificates for authentication can understand what target at which to aim in building PKI-related capabilities into both new and legacy applications. And, of course, governmental entities that adopt the VOLT primary policy components as their own policies for issuing certificates will have a much easier time in negotiating to use the Commonwealth's cross-certification bridge, should the bridge prove useful to them. When VOLT open standards are the basis of more than one PKI, the task of mapping policy between them is simplified, and the bridge becomes an easy means of providing interoperability, if and when the applications involved understand how to deal with cross-certification.

The VOLT environment will be particularly useful for issuing certificates to citizens, who in turn may use them to reduce the redundant work of providing identity information about themselves to every governmental entity with which they interact.

Representative Virginia citizen Jane Smith has heard that she needs a VOLT Certificate to accomplish certain transactions via the Internet with state government offices. Although she can still visit—in person—each governmental office that provides a useful service to her, she has learned that she can save significant time and money online. However, for some (not all) transactions, she needs to have established in advance a "digital identity" that the government's computing systems can recognize.

This digital identity's potential uses are widespread. Within government, Jane may file online individual or business tax returns without the requirement of keeping handwritten signatures on file, register to vote online (and perhaps vote online, as well), apply for professional licenses and enroll her children in school over the Internet from home, securely sign electronic correspondence, and electronically request copies of such documents as marriage licenses and deeds. She also may use her digital identity to gain access to the information that the Commonwealth keeps in its records about her to ensure that it is accurate. And, because a digital signature when properly implemented provides the identity-assurance functions of a notary public and can more completely ensure that a document has not been altered after it has been signed, she can use it to sign contracts, wills and other legal documents.[1]

Jane, like all persons using a PKI environment, must understand and accept her responsibilities, most notably the responsibility to safeguard the "private key" that remains in her personal possession. The focal point of vulnerability in any PKI environment is the user's private key, which in this case is hidden from Jane's view either in a file on her computer or on a hardware token such as a smartcard or an i-button and which in turn generated the public key that is a critical piece of her VOLT Certificate. Jane must learn that her password or PIN, which she'll have to know when using this technology, is something she should protect and not share with anyone else. The private key location and the password/PIN are roughly the equivalents of the bankcard and PIN that Jane uses at automated teller machines when she needs cash. She must do her best to ensure that persons she does not trust do not have access to her private key's physical location, and she needs to make sure she does not share or carelessly expose her password/PIN with others.

The VOLT Certificate program, part of the VOLT open standards PKI environment, in its earliest implementation gives its users—especially the citizens of Virginia—significant benefits by:

- Providing a single process for acquiring the personal digital certificate that allows Virginians to interact with Virginia government, including all of its participating agencies and institutions, online in highly secure fashion, protecting both the interests of the individual and the interests of government.
- Offering a solution that works with existing hardware and software tools.
- Producing a personal digital certificate inexpensively, making it feasible for the process to be repeated (a new certificate issued) whenever needed.
- Reducing complexity in the underlying PKI components to manageable levels, simplifying audit issues and increasing confidence for all parties.
- Allowing governmental certification authorities to rely on certificates produced by both vendor products and open-source software, as long as they are produced in conformity with straightforward, understandable standards.

Enabling non-governmental entities to use the VOLT Certificate as an online identification aid, although those entities will not have access to the address and other personal information that may be available to participating state agencies.

[1] Nearly all of these uses will require changes in law or in regulations.

APPENDIX N

INTERNAL CONTROL AND AUDITING STANDARDS

By Audit & Assurance Team
August 15, 2000

INTRODUCTION

This section of the report will discuss internal control, and audit standards in some detail, as they relate to public key infrastructure.

Internal controls and standards: “Internal control” refers to a general set of guidelines and procedures designed to detect and/or prevent (a) unintentional mistakes from occurring, or (b) intentional misappropriation or other types of undesirable results (e.g., stealing money or misusing digital signature certificates). An organization’s management is responsible for designing or implementing internal control procedures to provide “reasonable assurance” of detection or prevention of the foregoing. The audit and accounting community has adopted the term “reasonable assurance” because it indicates that no internal control can be absolutely 100% effective (due to the possibility of collusion, among other things), and also because 100%-effective internal controls are almost always cost prohibitive to implement (cost exceeds their benefit).

To aid management in determining what types of internal controls an organization should adopt for any given process, there are standards. “Standards” are a set of guidelines, which any of a number of accounting, auditing, or other group might promulgate through a consensus process, that set forth agreed-upon ways to do things. For example, “generally accepted accounting principles” (GAAP) sets forth the ways in which organizations should account for their finances, which ensures that financial results are comparative between distinct organizations.

The audit subcommittee performed an exhaustive search for published standards that would help management in establishing the appropriate internal controls for the Commonwealth’s digital signature effort. The subcommittee found that digital signature technology is emerging at the time of this report; therefore, there are very few published audit and control standards tailored specifically to digital signatures. The American National Standards Institute (ANSI) has taken a lead role in developing standards for the digital signature arena, having issued two standards that are directly applicable to auditing, in addition to a plethora of very specific technical standards. Although the ANSI organization created these standards for the financial community, they are largely applicable to the governmental environment as well.

Generally speaking, the standards discussed within this report are organized according to control objectives (what the control is intended to prevent or accomplish) and control procedures (the steps taken in actually implementing the control, e.g., daily reconciliation of cash collected). This report will provide a brief overview of the necessary controls, and the applicable standards that the audit subgroup recommends for management to use to provide guidance in establishing these controls.

Audit standards: For the purposes of this report only, “audit standards” are generally accepted (among the audit and accounting community) ways that an organization’s management can gather objective assurance that the proper internal control guidelines and procedures are in place and being properly followed. Organizations most commonly choose to gather this assurance by using an objective internal audit function.

There is also a myriad of audit standards, generally speaking. This report will identify, to the extent possible, a brief overview of audit standards that would help an appropriately objective audit function to provide reasonable assurance regarding internal control presence and function.

INTERNAL CONTROLS

INTERNAL CONTROL FRAMEWORK

Many distinct internal control procedures and guidelines will work together to create the control framework. An organization’s management is responsible for putting the control framework into place to help ensure that PKI using digital signatures accomplishes the following:

1. performs as intended;
2. safeguards electronic information for the required retention period, in a manner easily retrievable for audit purposes, and secured from unauthorized access;
3. safeguards individuals' digital certificates from unauthorized use;
4. detects unauthorized digital signature certificate use, or other attempted security breaches.

There are three parts of the PKI where specific internal controls will be present: the registration authority (RA), the certificate authority (CA) and the end-user. The controls that would govern the information flow between two or more of these groups (e.g., a verified certificate) are contained within one of the three groups listed, and are not listed separately for purposes of this report.

Registration authority internal controls would include the following non-exhaustive list:

- procedures to ensure that the level of identification verification is appropriate for the level of activity or risk associated with someone's certificate; and
- procedures to ensure that a copy of identification verification submitted is retained for an appropriate amount of time, in a readily-retrievable fashion, secured from unauthorized access.

Certificate authority internal controls would include the following non-exhaustive list:

- procedures to ensure that systems, physical, and environmental security are functioning as required, to prevent intentional misappropriation of information or unintentional information disclosures or breaches;
- procedures to provide reasonable assurance that key management and certificate management events are completely and accurately logged.
- procedures designed to provide reasonable assurance that the CA is employing proper key management techniques, designed to safeguard critical key information.

End-user internal controls would include the following non-exhaustive list:

- procedures over software, hardware, and human interaction to adequately ensure the security of a person's digital signature. These procedures would vary according to the level of risk associated with misappropriation of the signature;
- procedures to ensure the overall security and control of an information system or network where digital signature is used; and
- procedures to ensure that retention of electronic documents is within the Commonwealth's document retention requirements, retained documents are kept securely, and are easily accessible when needed.

INTERNAL CONTROL STANDARDS

REGISTRATION AND CERTIFICATE AUTHORITY CONTROL STANDARDS

ANSI X9.79 standard (American National Standard for Financial Services – "PKI Practices and Policy Framework" (ASC X9.79)) contains control objectives (what a control is designed to accomplish or protect) and control procedures (how an entity puts a particular control into operation) for many facets of certificate authority operations. The standard also includes a table with control procedures for registration authorities (see ASC X9.79, Table B-24, "Control Procedures – Subscriber Registration").

ANSI X9.79 provides the following non-exhaustive listing of control objectives and procedures, and refers the reader to other ANSI standards that could apply to their PKI implementation:

- *systems, physical, and environmental security control objectives* and procedures, which provide guidance in establishing controls to prevent the intentional information misappropriation or unintentional information disclosures. ANSI X9.79 accomplishes this by, among other things, providing very specific guidance in terms of personnel practices, third party access security, creation of clearly-defined physical security perimeters, protection of equipment from any sort of mechanical or other failure, and incident reporting and handling.
- *event log control objectives*, which provide guidance in establishing logs for critical activity, such as key management, and certificate management events; and

- *key management control objectives*, which provide guidance to the CA to enhance the trust environment by ensuring proper management and control over managing private and public key generation and distribution.

As of the date of this report, the ANSI X9.79 standard was in **DRAFT FORMAT**; however, the audit subcommittee does not expect any changes in the final version to impact significantly the broad discussion of ANSI X9.79 contained within this report.

The ***ANSI X9.49 standard*** (American National Standard for Financial Services – "Secure Remote Access to Financial Services for the Financial Industry") provides several useful control standards applicable to the Commonwealth's digital signature initiative. Specifically, the X9.49 standard provides a useful discussion of the certificate life cycle.

There are many other additional ANSI standards, the scope and specificity of which are beyond the scope of this report. ANSI X9.49 and X9.79 contain an exhaustive listing of them.

RECOMMENDATION: Because the ANSI X9 standards provide an exceptional control framework for PKI and digital signatures, the audit subcommittee recommends their use.

END-USER CONTROL STANDARDS

The end-user community is comprised of those individual or governmental agency entities that will ultimate rely on certificates either to provide their attestation in e-commerce, or as an attestation from an unrelated party in e-commerce. As of the date of this report, there was no single source of control standard guidance, tailored specifically for digital signature technology, published for the end-user community.

The "Control Objectives for Information and related Technology" (COBIT) (published and copyrighted by the Information Systems Audit and Control Foundation (ISACF)) provides generally accepted standards for IT security and control practices. The book entitled Digital Signatures – Security and Control, published by the ISACF, contains a broad example of using COBIT to establish good IT security and control practices (see Chapter 7).

RECOMMENDATION: The audit committee recommends the use of both of these documents in crafting audit standards for digital signature applications.

Arguably the most important issue affecting end-user controls is the security over end-user access to digital signing capability. The positive link between a digitally signed document and its signer is essential in supporting non-repudiation, which in turn is crucial to the digital signature trust environment.

ANSI X9.49 refers to end-user security access in terms of "identity factors," and lists three of them, in order of the level of security that each respectively provides:

- *knowledge factor* (information a person retains in memory – password);
- *possession factor* (information on an object that a person possesses, such as a smart card); and a
- *biometric factor* (information based on physical characteristics, such as a thumbprint).

A combination of the factors is generally more secure than any single factor alone. The strongest factor combination would be knowledge and biometric factors, whereas the weakest combination would be knowledge and possession factors. (KPMG seminar entitled "Commonwealth of Virginia – Audit Issues Seminar," presented by Jeff Stapleton).

There is a cost/benefit component to selecting the appropriate identity factor for each individual end-user, which would compare the value of the information (or signature capability) that could be potentially misappropriated with the cost of providing the factor.

RECOMMENDATION: As end-users bring e-commerce systems on-line using digital signature technology, the audit subcommittee recommends that the end-users perform a cost/benefit and risk analysis to select the appropriate identity factor(s) that each user, in each application, would use.

APPENDIX N

AUDIT STANDARDS

For the purposes of this report, an *audit framework* is an independent and objective assurance activity designed to help ensure that organizations accomplish their objectives for digital signature activity by using a systemic approach to evaluate and improve the effectiveness of risk management, and control processes. There are several documents that provide guidance in this area.

REGISTRATION AND CERTIFICATE AUTHORITY STANDARDS

The American Institute of Certified Public Accountants (AICPA) and the Chartered Accountants of Canada (CA) have published ***CA WebTrust*** (Exposure Draft AICPA/CA WebTrust $^{SM/TM}$ Principles and Criteria for Certification Authorities, Version 1.0 2/9/2000). **This document is in draft form as of the date of this report**. *WebTrust* provides an exhaustive framework for licensed *WebTrust* practitioners, who would likely be Certified Public Accountants, to use in assessing the adequacy and effectiveness of the controls for certificate authorities. *WebTrust* provides the auditor with a crosswalk for evaluating compliance with the X9.79 standard and suggested report wording for communicating that the entity has complied. By way of reference, *WebTrust* also provides some controls applicable for registration authorities.

RECOMMENDATION: Regardless of whether the Commonwealth ultimately decides to outsource the certificate and/or registration authorities, or keep them "in-house," the audit subcommittee strongly recommends that the CA (or multiple CA's) selected create a control structure sufficient to receive the *WebTrust* seal. Each CA should obtain the seal from an appropriately qualified practitioner. This seal provides a critical level of assurance that will help to ensure the success of digital signature-based technology in the Commonwealth.

Nearly all audits begin with determining completing some sort of "risk assessment" model, which attempts to evaluate each component of a digital signature environment for the risk that the component will fail to operate properly. Since no audit organization can audit 100% of any system, or all systems, the risk assessment guides auditors in determining how much audit effort they should expend, and the areas in which they should expend it.

RECOMMENDATION: The ***ANSI X9.49 standard*** provides an excellent risk analysis methodology that would be useful in helping to determine audit risk. The risk analysis in the standard is used in the form of a "security requirements matrix," which determines the relative levels of several security features; e.g., level and type of identity authentication credentials needed. The risk analysis provides a methodology for rating risk using four primary risk factors: monetary loss, productivity loss, embarrassment, and legal liability.

END USER AUDIT STANDARDS

As of the date of this report, an audit framework for digital signature technology, targeted for the end-user community, did not exist. However, the audit committee formulated recommendations with respect to the structure and frequency of audit activity involving digital signature technology.

In the audit committee's view, an agency's assurance function should provide periodic testing of end-user access controls, as well as the storage and indexing of electronic information (such as contracts). The success of the internal controls in these end-user functional areas is absolutely critical to the success of e-business in the Commonwealth. Without the appropriate controls over access to individual PC's storing digital certificates, the potential for misuse of signatory authority, or repudiation of any digital "document" is substantial. If the Commonwealth encounters a situation where certificate holders are repudiating what was sent under their digital signature, this has the potential to severely undermine the effectiveness of the entire e-business system relying on digital signature technology.

In terms of electronic information storage and indexing, for every manual paper system that an electronic system replaces, there are still electronic "documents" that organizations need to retain for audit purposes, as well as for state storage requirements. Periodically, internal or external auditors test financial statement accuracy by tracing back through accounting transactions that occurred in the past. The electronic source "documents" are essential to perform these tests so that ultimately, external auditors may attest to the accuracy of financial statements on a yearly basis. Without proper retention schedules, documents vital to the Commonwealth's business operations may be lost. Without adequate indexing of these electronic documents, organizations may not be able to "find" the documents when they need to access them. The lack of a good indexing system is analogous to storing paper documents in a massive file drawer without any sort of file tabs or other mechanism to find the files.

RECOMMENDATION: Each end-user agency or institution should establish an assurance function that would examine PKI applications on an appropriate schedule, following guidance provided by COTS or its PSA workgroup. The frequency of audits that the assurance function would perform would be dependent upon the risk associated with digital signature technology in each organization. Some possible entities that might conduct this assurance function include: the existing agency internal audit function, a contractor, or other qualified individual independent from the group responsible for implementing and managing the agency's PKI application.

RECOMMENDATION: Appendix 3, Digital Signatures – Security and Controls, contains an audit program, portions of which are useful in crafting an audit program for the end-user community. Chapter 4 of the same publication contains brief explanations of various security risks, some of which apply to the end-user community as well.

RECOMMENDATION: The Commonwealth should provide agencies and institutions with adequate training and technical support to assure proper management of PKI function. The Commonwealth should provide periodic quality assurance reviews of agencies' PKI assurance function, as well as craft a bank of audit tests that agencies' assurance functions could use on a recurring basis. This would ensure that the quality of PKI assurance functions remains relatively constant among state organizations, providing an additional degree of trust in digital signature technology. The Commonwealth should consider whether to request that outside service providers obtain a SAS 70 review.

RECOMMENDATIONS SUMMARY

As of the date of this report, the preponderance of standards specifically tailored for control and audit frameworks in the digital signature environment is germane to certificate authorities, and to a lesser degree to registration authority operations. From an audit and controls perspective, the audit subcommittee recommends the following, which will contribute greatly to the success of digital signature technology statewide:

- Use ANSI X9 standards in crafting the internal control framework for digital signature technology.

- Use "Control Objectives for Information and related Technology" (COBIT) in establishing security and control practices for end-user applications, as well as for certificate and registration authorities.

- End-users should conduct a cost/benefit and risk analysis to select the appropriate identity factor(s) for accessing each person's digital signature application. ANSI X9.49 contains a listing of these factors.

- Whether the Commonwealth outsources or provides certificate authority services itself, the certificate authority should create a control structure sufficient to obtain the *WebTrust* seal, and should obtain the seal from a qualified practitioner.

- To help in determining audit risk of digital signature systems, agencies' audit functions should consult and strongly consider the use of ANSI X9.49.

- Each end-user agency or institution should establish an assurance function that would examine PKI applications on an appropriate schedule, following guidance provided by COTS or its PSA workgroup.

- The Commonwealth should provide agencies and institutions with adequate training and technical support to assure proper management of PKI functions. The Commonwealth should provide periodic quality assurance reviews of agencies' PKI assurance function, as well as a bank of audit procedures that individual state organizations could use in performing their assurance reviews.

APPENDIX O

COMPARISON OF ELECTRONIC SIGNATURE LEGISLATION

By Michie Longley, Department of Motor Vehicles
October 16, 2000

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (FEDERAL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (NCCUSL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (VIRGINIA – HR 499)	
TITLE I — ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE				CHAPTER 43 — UNIFORM ELECTRONIC TRANSACTIONS ACT	
SECTION	PROVISIONS	SECTION	PROVISIONS	SECTION	PROVISIONS
Section 101 (a)	**GENERAL RULE OF VALIDITY:** Establishes legal effect, validity and enforceability of electronic contracts, formats and signatures.	Section 7	**LEGAL RECOGNITION:** Essentially the same as the federal law. Establishes that electronic records, signatures and contracts may not be denied legal effect or enforceability.	§ 59.1-507	**LEGAL RECOGNITION:** Essentially the same as the federal law. Establishes that electronic records, signatures and contracts may not be denied legal effect or enforceability.
Section 101 (b)	**GENERAL RULE OF VALIDITY:** Title pertains only to electronic provisions and does not limit or alter other requirements and obligations. It does not require any person to use or accept electronic records or signatures.	Section 5	**USE OF ELECTRONIC RECORDS AND SIGNATURES:** Does not mandate use of electronic records or signatures. Provisions pertain only to those parties who have agreed to conduct electronic transactions.	§ 59.1-505	**USE OF ELECTRONIC RECORDS AND SIGNATURES:** Does not mandate use of electronic records or signatures. Provisions pertain only to those parties who have agreed to conduct electronic transactions.
Section 101 (c) (1)	**CONSUMER DISCLOSURES — CONSENT:** Consumer must affirmatively consent to accept electronic transactions. Consumer rights must be conspicuously posted. Consumer must be informed of: • Rights to receive record in non-electronic form • Right to withdraw consent • What is actually being consented to (this transaction or all future transactions) • Fees and hardware/software requirements • Changes in fees and hardware/software requirements Finally, consumer must consent electronically in such a way that demonstrates the ability to receive and access electronic records.	— N/A —	No comparable sections; however, such consumer disclosures are not prohibited. Section 5 allows a person who agrees to an electronic transaction to refuse other electronic transactions. This particular provision cannot be waived by agreement	— N/A —	No comparable sections; however, such consumer disclosures are not prohibited. § 59.1-505 (c) allows a person who agrees to an electronic transaction to refuse other electronic transactions. This particular provision cannot be waived by agreement.

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (FEDERAL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (NCCUSL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (VIRGINIA – HR 499)	
TITLE I — ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE				CHAPTER 43 — UNIFORM ELECTRONIC TRANSACTIONS ACT	
SECTION	PROVISIONS	SECTION	PROVISIONS	SECTION	PROVISIONS
Section 101 (c) (2)	**OTHER RIGHTS:** Nothing in this law affects content or timing of consumer disclosure required by other laws.	— N/A —	No comparable sections; however, such consumer disclosures are not prohibited.	— N/A —	No comparable sections; however, such consumer disclosures are not prohibited.
Section 101 (c) (3)	**FAILURE TO OBTAIN CONSENT:** Legal validity of an electronic contract will not be denied solely because of failure to obtain electronic consent.	— N/A —	No comparable sections; however, such consumer disclosures are not prohibited.	— N/A —	No comparable sections; however, such consumer disclosures are not prohibited.
Section 101 (c) (4)	**CONSUMER DISCLOSURES — PROSPECTIVE EFFECT:** Withdrawal of consent does not invalidate the legality of electronic records and contracts made while consent was in effect.	— N/A —	No comparable sections; however, such consumer disclosures are not prohibited.	— N/A —	No comparable sections; however, such consumer disclosures are not prohibited.
Section 101 (c) (5)	**PRIOR CONSENT:** Excludes from these provisions any records provided to consumers who consented to electronic records prior to the effective date of this law.	Section 4	**PROSPECTIVE APPLICATION:** Provisions apply to records and contracts created, generated, sent, etc., on or after the effective date of this law.	§ 59.1-504	**PROSPECTIVE APPLICATION:** Provisions apply to records and contracts created, generated, sent, etc., on or after the effective date of this law.
Section 101 (c) (6)	**ORAL COMMUNICATIONS:** These are not considered electronic records.	— N/A —		— N/A —	
Section 101 (d) (1) & (2)	**RETENTION OF CONTRACTS AND RECORDS:** Where statutes or regulations, etc., require records to be retained, allows them to be kept in electronic format, so long as • The record accurately reflects the information contained in the record or contract, and • The electronic record remains accessible to all who are entitled to access it.	Section 12	**RETENTION OF ELECTRONIC RECORDS:** Essentially the same as the federal law. If law requires records to be retained, allows them to be kept in electronic format. Also allows use of third party to provide services so long as all requirements are met.	§ 59.1-512	**RETENTION OF ELECTRONIC RECORDS:** Essentially the same as the federal law. If law requires records to be retained, allows them to be kept in electronic format. Also allows use of third party to provide services so long as all requirements are met.

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (FEDERAL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (NCCUSL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (VIRGINIA – HR 499)	
TITLE I — ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE				CHAPTER 43 — UNIFORM ELECTRONIC TRANSACTIONS ACT	
SECTION	PROVISIONS	SECTION	PROVISIONS	SECTION	PROVISIONS
Section 101 (d) (3)	**ORIGINALS:** Allows electronic formats where statutes or regulations, etc., require interstate or foreign contracts or records to be retained in original form.	Section 12	Same as federal law.	§ 59.1-512 (d)	Same as federal law
Section 101 (d) (4)	**CHECKS:** Allows electronic record of the information on the front and back of a check where statutes or regulations, etc., require the check to be retained.	Section 12	Same as federal law.	§ 59.1-512 (e)	Same as federal law.
Section 101 (e)	**ACCURACY AND ABILITY TO RETAIN CONTRACTS AND RECORDS:** Legal effect, validity and enforceability of an electronic contract or record may be denied if the electronic version cannot be later accurately reproduced.	Section 8	**PROVISION OF INFORMATION:** While worded differently from the federal law, the effect is the same. If an electronic record is not capable of being retained by the recipient, the electronic record cannot be enforced against the recipient.	§ 59.1-508	**PROVISION OF INFORMATION:** While worded differently from the federal law, the effect is the same. If an electronic record is not capable of being retained by the recipient, the electronic record cannot be enforced against the recipient.
Section 101 (f)	**PROXIMITY:** This law does not remove responsibility to maintain warnings, notices, disclosures, etc., required by law.	— N/A —	No comparable section.	— N/A —	No comparable section.
Section 101 (g)	**NOTARIZATION AND ACKNOWLEDGMENT:** An electronic signature by an authorized person (such as a notary) satisfies the requirement where notarization, acknowledgment, etc., is required by law, statute or regulation.	Section 11	Same as federal law.	§ 59.1-511	Same as federal law.
Section 101 (h)	**ELECTRONIC AGENTS:** Establishes the validity of an electronic contract involving an electronic agent. Electronic agent is defined as a computer program or other such automated means used to initiate an action.	Section 14	**AUTOMATED TRANSACTIONS:** Provides that contracts can be established through electronic agents.	§ 59.1-514	**AUTOMATED TRANSACTIONS:** Provides that contracts can be established through electronic agents.

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (FEDERAL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (NCCUSL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (VIRGINIA – HR 499)	
TITLE I — ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE				CHAPTER 43 — UNIFORM ELECTRONIC TRANSACTIONS ACT	
SECTION	PROVISIONS	SECTION	PROVISIONS	SECTION	PROVISIONS
Section 101 (i)	**INSURANCE:** Specifies that the provisions of this law apply to the business of insurance.	— N/A —		— N/A —	
Section 101 (j)	**INSURANCE AGENTS AND BROKERS:** Specifies liabilities that may apply under electronic insurance contracts.	— N/A —		— N/A —	
Section 102 (a) (1) & (2)	**EXEMPTION TO PREEMPTION:** Spells out conditions under which state statutes and regulations may modify, limit or supersede this law. These include: • Enactment/adoption of NCCUSL's UETA so long as they are not in conflict with this law, or • Specification of alternative procedures or requirements for electronic records and signatures, without requiring the implementation of a specific technology.	— N/A —		— N/A —	
Section 102 (b)	**EXCEPTIONS FOR ACTIONS BY STATES AS MARKET PARTICIPANTS:** Excludes laws governing procurement by states.	— N/A —		— N/A —	
Section 102 (c)	**PREVENTION OF CIRCUMVENTION:** Nothing in subsection a allows a state to circumvent this law.	— N/A —		— N/A —	

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (FEDERAL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (NCCUSL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (VIRGINIA – HR 499)	
TITLE I — ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE				CHAPTER 43 — UNIFORM ELECTRONIC TRANSACTIONS ACT	
SECTION	PROVISIONS	SECTION	PROVISIONS	SECTION	PROVISIONS
Section 103 (a) & (b)	**EXCEPTIONS:** Specifies when this law does not apply. These include: • Wills, codicils, trusts • Adoptions, divorces • Uniform Commercial Code • Court orders, notices, official documents • Notices of cancellation of utility services • Defaults, repossessions, foreclosures • Cancellations/terminations of health benefits • Product recalls • Hazmat documents	Section 3	**SCOPE:** Excludes wills, codicils and trusts; the Uniform Commercial Code (except for specified sections dealing with waivers after breach of contract, certain frauds, sales, and leases). Does not prohibit the other exemptions provided in federal law.	§ 59.1-503	**SCOPE:** Excludes wills, codicils and trusts; the Uniform Commercial Code (except for specified sections dealing with waivers after breach of contract, certain frauds, sales, and leases). Does not prohibit the other exemptions provided in federal law.
Section 103 (c)	**REVIEW OF EXCEPTIONS:** Provides for review, findings and decision on changes to exceptions.	— N/A —	No comparable section.	— N/A —	No comparable section.
Section 104 (a)	**APPLICABILITY TO FEDERAL AND STATE GOVERNMENTS:** Except for federal paperwork reduction act, allows regulatory agencies to continue established formats and process required for filing records.	— N/A —	No comparable section.	— N/A —	No comparable section.

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (FEDERAL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (NCCUSL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (VIRGINIA – HR 499)	
TITLE I — ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE				CHAPTER 43 — UNIFORM ELECTRONIC TRANSACTIONS ACT	
SECTION	PROVISIONS	SECTION	PROVISIONS	SECTION	PROVISIONS
Section 104 (b)	**RULEMAKING AUTHORITY:** Rule making agencies may interpret this law as it pertains to issuance of regulations, orders and guidance, so long as they • Are consistent with this law • Do not add to the requirements of this law • Do not impose methods that are substantially different from that used for paper records • Do not impose unreasonable costs. Also sets performance standards and allows regulatory agency to determine when paper records are required.	— N/A —	No comparable section.	— N/A —	No comparable section.
Section 104 (c)	**ADDITIONAL LIMITATIONS:** Prohibits reimposition of paper records.	— N/A —	No comparable section.	— N/A —	No comparable section.
Section 104 (d)	**AUTHORITY TO EXEMPT:** Allows federal regulatory agency to exempt class of records from the consumer consent requirements of this law.	— N/A —	No comparable section.	— N/A —	No comparable section.
Section 104 (e)	**ELECTRONIC LETTERS OF AGENCY:** Specifies that FEC must accept electronic records and signatures.	— N/A —	No comparable section.	— N/A —	No comparable section.
Section 105 (a) & (b)	**STUDIES:** Mandates studies by Secretary of Commerce.	— N/A —		— N/A —	
Section 106	**DEFINITIONS**				

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (FEDERAL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (NCCUSL)		UNIFORM ELECTRONIC TRANSACTIONS ACT (VIRGINIA – HR 499)	
TITLE I — ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE				CHAPTER 43 — UNIFORM ELECTRONIC TRANSACTIONS ACT	
SECTION	PROVISIONS	SECTION	PROVISIONS	SECTION	PROVISIONS
Section 107 (a) & (b)	**EFFECTIVE DATE:** Effective 10/1/2000 with following exceptions: • **Records Retention:** Effective 3/1/2001 for all regulatory or statutory requirements for records to be retained • **Pending Records Retention:** Effective 6/1/2001 for any pending rules announced or proposed on or by 3/1/2001 by a federal or state regulatory agency • **US Loans:** Effective one year after enactment for US Government guaranteed and insured loans • **Student Loans:** Effective when the Secretary of Education publishes revised promissory notes, or one year after enactment of this law (whichever is earlier).	— N/A —			7/1/2000

APPENDIX P

LEGISLATIVE ENVIRONMENT

By Audit & Assurance Team
August 7, 2000

NEW LEGISLATION

During the past year, both the Federal and State governments have passed significant legislation related to the conduct of business electronically including the use of electronic signatures. On March 14, 2000 Governor Gilmore signed the nation's first Uniform Computer Information Transactions Act (UCITA). He signed one of the nation's first Uniform Electronic Transactions Act (UETA) shortly thereafter. On June 30, 2000, President Clinton signed the Electronic Signatures in Global and National Commerce Act (E-Sign Law).

It is important to note there is significant overlap between the federal E-Sign Law and the Commonwealth's UETA. Though the Federal E-Sign Law contains provisions for preemption of State Laws, there are caveats to the preemption that must be evaluated such as a caveat regarding non-uniform provisions. Further, despite the overlap in the Federal and State legislation, the scopes of the two pieces of legislation are not identical. For example, there is a second group of items excluded from E-Sign that do not have a parallel in UETA such as cancellation or termination of utility services, of health insurance or benefits or life insurance benefits as well as notices of default, acceleration, repossession, foreclosure, eviction, or right to cure a credit agreement or a rental agreement relating to a primary residence and notice of recall or material failure of a product which might endanger health or safety. Finally, any document required to accompany the shipping or handling of hazardous or toxic materials is excluded.

It is equally important to note the legislation is new and few precedents are available to guide the formulation of e-government policies and best practices within the Commonwealth. The interpretation of these legislative efforts within the courts will be a deciding factor in their validity. Further, the exponential growth of technology and related evolving business practices have placed legislation at every level - global, federal, state and local in a reactionary mode.

Consequently, it is of paramount importance to the success of digital signatures, specifically, and e-government in general to have expert legal advice in formulating optimal policies, procedures and practices. **To this end, we recommend the Commonwealth consider providing resources to establish an e-commerce section within the Office of the Attorney General.**

The Virginia versions of both UCITA and UETA were based on the models promulgated by the National Conference of Commissioners on Uniform State Laws (NCCUSL).

UCITA, which is modeled after the Uniform Commercial Code, Article 2, is designed to govern transactions of computer information and becomes effective July 1, 2001. In the interim, UCITA directs the Joint Commission on Technology and Science to study the impact of UCITA and report its findings to the Governor and General Assembly by December 1, 2000. Amendments to the UCITA model have been proposed and will be considered at the NCCUSL 2000 Annual Meeting Draft July 28, 2000-August 4, 2000.

UETA (§ 59.1-479 et. seq.) has a more material impact on the deployment of digital signatures in the Commonwealth as it is broader in scope than UCITA, is directly related to electronic signatures, and was effective July 1, 2000. UETA repealed existing Virginia laws on electronic signatures and electronic filings while incorporating some of the previous provisions, such as the exemption for the court filings and making technical amendments throughout the Code to conform to the provisions of UETA.

Under UETA, the Commonwealth's requirements for admissibility of electronic signatures as evidence remain essentially the same as in the rescinded Code section (§ 59.1-468) as follows

"§ 59.1-491 Admissibility of Evidence . . .b. In determining the evidentiary weight to be given a particular electronic signature, the trier of fact shall consider whether the electronic signature is:

(i) unique to the signer,
(ii) capable of verification,

(iii) under the signer's sole control,
(iv) linked to the record in such a manner that it can be determined if any data contained in the record was changed subsequent to the electronic signature being affixed to the record, and
(v) created by a method appropriately reliable for the purpose for which the electronic signature was used.

The trier of fact may consider any other relevant and probative evidence affecting the authenticity and/or validity of the electronic signature."

However, UETA rescinded the previous Code requirement that restricted State officials to using "electronic" signatures only when the five specific criteria contained in the admissibility section were met. The previous requirement arguably restricted state officials to accepting only digital signatures in a PKI environment even when simpler, less costly signing methods may have sufficed. Alternatively, UETA contains provisions that allow state officials to exercise discretion regarding the types of electronic signatures to require based on the characteristics of the particular type of transaction under the oversight of the Secretary of Technology.

LEGISLATIVE OPPORTUNITIES

Despite the legislative progress the federal government and the Commonwealth have made in the electronic signature arena, there are ~~may be~~ certain issues vital to the successful deployment of digital signatures that have yet to be addressed. With the use of digital signatures, the certificate authority is the trusted third party that vouches for the identities of holders of certificates that it issues and is responsible for maintaining current and accurate records related to the issued certificates including whether the certificate is valid or revoked. Consequently, the credibility of the certificate authority is paramount in providing the features of authentication, integrity and non-repudiation and, therefore demands a high level of reliability. The level of trust and reliability that will be placed on CA's tomorrow may be analogous to the level of trust and reliance currently placed on banks and other financial institutions today.

Issues such as the CA's level of liability or immunity from liability, responsibility for security and confidentiality, and standards for translating accurately varying levels of authentication are as yet unresolved. Currently, no specific federal or Commonwealth statutes address regulation of certificate or registration authorities. The standards and best practices for certificate authorities are still evolving. Some countries such as Singapore and some states such as Washington have chosen to legislate licensing of CA's. The service providers advocate an approach of market driven self-regulation. Canada, in October 1998, announced its cryptography policy that included the determination it would not regulate private sector entities providing authentication and certification services. Alternatively, the Industry Canada's Electronic Commerce Branch in July 2000 issued a paper titled "A Framework for Electronic Authentication in Canada" in which an Accreditation Model is proposed.

Given the relatively neophyte stage of the CA issues, we recommend that evolving international, national and state legislation and practices be monitored and that existing legislation be studied to determine whether germane issues, such as CA liability and security are addressed fully.

A critical element of a secure PKI and digital signature implementation is the ability to maintain confidentiality over certain key components such as user authentication information, private or secret keys, security architecture, any passwords or other access systems utilized. In the Commonwealth, as in most government environments, all public records are required to be open to inspection by any citizens and others, except as otherwise specifically provided by law. In our review of the Virginia Freedom of Information Act (VFOIA) we noted the following exclusion that appears adequate to allow confidential components of a PKI and related digital signatures to be withheld from public inspection.

"§ 2.1-342.01. Exclusions to application of chapter.
A. The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law: . . .
45. Documentation or other information which describes the design, function, operation or access control features of any security system, whether manual or automated, which is used to control access to or use of any automated data processing or telecommunications system."

xxv.

It should be noted that exclusions under VFOIA such as this allow a public official to choose not to release the applicable records rather than prohibiting the disclosure.

Though the exclusion appears to be adequate, since our interpretation of the exclusion is not from a legal representative, we recommend that the Office of the Attorney General be requested to advise whether this exclusion provides adequate protection for the confidential components of Commonwealth PKI and digital signature processes.

POTENTIAL LEGAL AND POLICY BARRIERS

There are also provisions within the existing Code of Virginia that specifically require manual processing such as the use of envelopes or certified or registered mail. A general search of the Code for certified mail disclosed 258 uses of the term in 216 documents.

Additionally, state agencies and institutions have promulgated regulations and policies based predominately on manual processes and, consequently, may pose barriers to implementing the Commonwealth's vision of e-government at a minimum and perhaps may also preclude the use of digital signatures.
The government of the Commonwealth is addressing identification of existing barriers to electronic government in several efforts. The Joint Commission on Technology and Science established an Advisory Committee in 1999 to study electronic government.

Senate Joint Resolution 72 directs the Auditor of Public Accounts, in consultation with the Department of General Services, to study whether audits of public accounts can be satisfactorily conducted with electronic contracting and electronic procurement processes and identify any statutory or regulatory barriers or obstacles which may prevent the implementation of electronic contracting and electronic procurement processes that are envisioned for the Commonwealth.

Executive Order 65(00) establishes the Electronic Government Implementation Division within the Department of Technology Planning. This division is charged with, among other things, with the cooperation and assistance of the Governor's Cabinet and the Council on Technology Services, to identify changes necessary to implement web-enabled versions of Executive Branch administrative systems that can be effected through policy directive, Executive Order, change in regulation, or amendment of the Code of Virginia.

To expedite the implementation of e-government, including digital signatures where applicable, we recommend the Electronic Government Implementation Division require each state agency, institution and political subdivision to review their existing Code sections, regulations, and policies to identify any statutory, regulatory or policy requirements that are potential barriers and to initiate the appropriate changes.

Finally the review process for agencies and institution's proposed new or revised regulations do not include a review to ensure that the regulations, to the extent practical, facilitate e-government including, where appropriate, the use of digital signatures

We also recommend Executive Order 25(98), which addresses the development and review of regulations, be amended to include language to ensure the proposed regulations enable, to the extent practical, electronic government and, where appropriate, digital signatures.

RESOURCES:

http://www.uetaonline.com/docs/pfry700.html
http://www.law.upenn.edu/bll/ulc/ulc.htm
http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+59.1-479
http://leg1.state.va.us/cgi-bin/legp504.exe?ses=001&typ=bil&val=hb499
http://leg1.state.va.us/000/lst/LS502105.HTM
http://leg1.state.va.us/000/lst/LS502057.HTM
http://leg1.state.va.us/000/lst/LS502076.HTM
http://jcots.state.va.us/adv_coms/2000/00_AC_3.htm
http://www.abanet.org/buslaw/cybernews/3-1ledig.html

APPENDIX Q

RFP RESOURCES

September 2000

DIGITAL SIGNATURE/DIGITAL CERTIFICATE SAMPLE QUESTIONS

BY DIGITAL SIGNATURE TRUST CO
AUGUST 29, 2000

DIGITAL CERTIFICATES:

- What levels of authentication, authorization, and non-repudiation are recommended for applications using purchasing transactions (including payments), email, electronic documents/forms, or general information type applications?
- How do State Agencies use digital certificates outside of using them for digital signatures? What if agencies or departments identify business requirements for digital certificates intended for encryption only? Or for single sign-on purposes?
- Is there a business requirement for Cross-Certification? Is Cross-Certification the answer to reciprocity with other states, Federal Government or with local governments? Explain policy issues surrounding this.

CERTIFICATE AUTHORITIES:

- How does the CA authenticate individuals for certificate registration or certificate request processing? (Methods for authenticating individuals)
- What are suggested guidelines for agencies or departments to follow when establishing agreements between CAs and subscribers and agencies or departments?
- What is an appropriate or acceptable level of variation from the Certificate Policy (CP) or Certificate Practice Statement (CPS)? Is this stated in either policy? If so, which one(s)?

STATEWIDE DIRECTORY:

- What information is recommended to be stored in the directory for digital certificates? (Examples of common information)
- Do the directories that support Digital Certificates interact with each other? If so, how do these directories interact with each other? What recognized standards apply?
- What can a State do with a statewide directory?
- Who is responsible for the storage, maintenance, and design of the directory?
- How do the directories interact or interface with legacy systems and data? Or do they?

POLICY ISSUES:

- How much detail should be included in the Certificate Policy (CP) with respect to types of transactions and the recommended rule sets for authorization or access to transactions?
- How do you address or adjust your CPS to align with a Certificate Policy (CP)? i.e. If two State Agencies have different CPs, how do adjust your CPS for each policy?
- Should the State write its own CP or adopt commercially acceptable CPs? Discuss the interoperability issues surrounding each option.
- Do you perform authentication of individuals? If so, what is the liability model?
- Do you support authentication by third parties? Again, what are the options and their associated liability models?
- What warranties and/or representations will your company make regarding delivery and performance of information assurance services?

GENERAL CAPABILITIES

- Do you validate certificates? If so, how?
- How do Relying Parties verify the certificate is valid in your service?

- Can it be used with a standard browser or is proprietary software required?
- What, if any, additional hardware is required by the State?

ADDITIONAL QUESTIONS

- Industry Standards Supported
    - X.509v3 standards, directory protocols, etc
- Reference Accounts
- Qualifications of the Vendor
- Implementation Plan
    - Time to market
- Integration Support (Professional Services)
- Service Levels Supported
- Customer Service
- Training and Training Materials
- Costs
    - One-time and recurring

SAMPLE RFP

BY RSA SECURITY, INC.
SEPTEMBER 5, 2000

SUPPLIER DELIVERABLES

In your response to this SOW, please include or address the following:

1. Contact person from your organization to address questions from <company> Evaluation Team. Please include name, title, telephone number, and e-mail address.
2. Company Questionnaire
3. Product & Services Questionnaire
4. Y2K Statement
5. Solution for paid Pilot Project
6. Recommendation for server hardware components to meet a continuous operation (24 X 7), scalability, manageability and reliability
7. Recommendation for software components to meet our stated needs for desktop security (power-up & file encryption), a secure e-commerce environment, secure e-mail, digital signatures and secure remote access.
8. Cost structure for a turnkey solution to include software licensing, on-site administrator and user training, technical consulting on design, implementation, integration (3rd party hardware/software/services) to achieve stated objectives, management cost of outsource CA solution and software maintenance. Break these costs out into one-time and recurring costs. Also indicate if there are any per-certificate costs.
9. Provide specifications for hardware items required to meet stated objectives and cost structure for hardware separate from item 8.
10. Summarized project plan (including timeline, software, hardware and personnel resources to install the technology into the <company> network and complete the remote access and e-mail pilot.)
11. Estimate of time, resources and professional services required to meet stated objectives.
12. Explain your contract licensing and provide a model contract including, but not limited to software licensing agreement, service agreement, and support agreement.
13. Is there anything that we have not asked about that you feel would be critical to our decision making process?

APPENDIX Q

COMPANY QUESTIONNAIRE

	QUESTION
1.	Name of Company: Street Address City State Zip Code Telephone Fax Internet Address
2.	Revenues (most recent figures available)
3.	Net profits after tax (most recent figures available)
4.	Legal Structure (Partnership, Corporation)
5.	Organization Chart (Please attach)
6.	Company Start Date
7.	Sales / Marketing Staff Levels
8.	Support Staff Levels
9.	Ratio of Customer Base to Support Staff
10.	Research & Development staff levels
11.	Research & Development Budget
12.	Location of Technical Support Facilities
13.	Percentage of revenues invested in R & D for all products in 1997, 1998 & 1999(projected)
14.	Turnover in the last 3 years Average Worldwide Average USA
15.	Are the personnel who authored the software still with the company?
16.	Is your company an authorized developer or partner with Microsoft Corporation? If yes, please explain.
17.	Is your company actively working with Microsoft Corporation on Windows 2000 technologies?
18.	Will there be any difficulty upgrading from the current shipping version of the software to future releases?
19.	How does your company differentiate itself from your competition?
20.	Have you had any false starts or situations where competitors replaced your product? If so why?

PRODUCT & SERVICES QUESTIONNAIRE

	Question
1.	Software Product Name
2.	Current Release / Version Available
3.	How long has this version been on the market?
4.	Date of release of original version

	Question
5.	Number of installed sites: Worldwide - USA -
6.	Development Language Used
7.	Projected Date of Next Release
8.	If applicable, please list major enhancements in next release
9.	Please provide 3 international/global companies as references that match our environment. All references must be using your current product. Include the following: • Contact Name & Title • Company Address & Phone • Approximate Annual Revenue • Industry • Hardware Configuration • Applications installed • Approximate number of users • Dates and releases installed • Modifications Made
10.	Can your desktop client (if available) support single sign-on to the network operating system: • Windows NT • Novell 3.x, 4.x, and 5.x Does this capability require any additional software or require an additional charge?
11.	Identify all the major software packages and technologies that your software will seamlessly integrate with (out of the box).
12.	List minimum and recommended hardware and network requirements for the following components of your solution: Clients: Windows 95 Windows 98 Windows NT
13.	Does your solution require installation of client software? If not, what mechanism is used to interface with applications, specifically non-web enabled applications?
14.	Can your product allow the recovery of encrypted files without the escrow of any private keys?
15.	Can your product allow automatic encryption/decryption of files on the local PC and network drives?
16.	When using automatic file encryption is all information encrypted over the network when accessing a file server? Is a plain text (decrypted) copy of the file ever created?
17.	Can your product create encrypted self-extracting executable files for sending encrypted information to users that do not have S/MIME complaint email clients and/or certificates?
18.	Is there any additional charge for file encryption capabilities?
19.	Does your product adhere to all the following standards? If not, which ones? • Certificates: X.509 v3, PKIX, etc. • Directories: X.500, LDAP, MS Active Directory • Other: S/MIME, SSL, IPSec
20.	How can your product PKI-enable applications where our company does not have the source code?
21.	Can your CA authenticate certificates from other vendors?
22.	Can your product be exported outside the US with full functionality?

	Question
23.	Which of the following algorithms are supported by client and server software? Asymmetric - Key Exchange RSA in accordance with PKCS#1 Symmetric – Bulk File Encryption
24.	Can your product work with multiple certificate authorities on an on-going basis? Which certification authorities can be used with your product?
25.	Can your CA be managed on either an in-house or outsource model?
26.	Is it difficult to migrate from an outsourced to an in-house solution if it becomes strategically beneficial?
27.	Per 1000 users, what are the anticipated manpower requirements for administering an in-house CA using your product (for a company with our given infrastructure and environment)? What is the anticipated manpower requirement for administering the RA for the in-house solution vs an outsourced solution, using your product?
28.	What is the average startup time for an in-house vs. outsourced solution with a company of our given infrastructure an environment?
29.	Describe the equipment and infrastructure requirements needed to securely operate an in-house CA based on your product (e.g., physical security, intrusion detection software, etc.)
30.	Are toolkits available to PKI-enable legacy and homegrown applications?
31.	How many people have your toolkits in their products?
32.	For what platforms can your toolkits be used to develop PKI interfaces?
33.	In what programming language(s) are your toolkits available?
34.	Provide one of more of your customers that has successfully utilized your toolkit to integrate an application and/or platform that was not "out of the box" PKI-ready. What application and/or platform was integrated?
35.	How do the following key and certificate management functions work in your product? a. Update of CA signing key pair and CA certificate Automatic update of user keypairs and certificates Automatic management of key histories Moving users between CAs Are decryption keys backed up centrally? Are signing keys backed up centrally? Can multiple authorizations be required for key recovery? When a certificate expires, is a new keypair issued? Or is the existing keypair renewed? How does your product use CRLs to determine certificate validity? Does your product support automatic revocation publishing and checking? Does your product support caching of CRLs? Immediate revocation checking?
36.	With your product, can a user use a single certificate to access all PKI-enabled applications and platforms?
37.	Does your certificate support the use of dual key pairs (encryption and signing), or would this require the issuance of two certificates?
38.	Describe the steps that a user and/or administrator typically would do to accomplish the following: b. Generate a certificate. c. Renew an expired certificate. d. Recover a key. e. Decrypt a file that was encrypted with an old keypair. f. How can your client software be distributed to large numbers of users?
39.	Does your product support multiple authentication factors, including passwords, SecurID tokens, and smart cards? Can you provide smart card readers and smart cards as well as the associated support and maintenance?
40.	Does your product support user roaming (i.e., secure storage of credentials on a central server)?
41.	If you product supports roaming users describe how fault-tolerance, load balancing, and redundancy is provided in the event of multiple catastrophic failures?

	Question
42.	How can you product be used to provide two-factor authentication via direct dial-up access?
43.	What directories does your CA support?
44.	Can your CA use cryptographic hardware for storage and signing?
45.	Does your CA support hierarchical cross-certification?
46.	Does your CA maintain audit logs? What activities can be logged? Are audit log entries timestamped? What kinds of reports can be generated by your product "out of the box"?
47.	Are there any functional limits on the number of users that your CA can support?
48.	Does your product support multiple remote Registration Authorities? Does your product support the capability for automated enrollment?
49.	Does your product support bulk loading of directories?
50.	Will your solution use or replicate to AD in Windows 2000 and, if so, how?
51.	When will the following components be ready for Windows 2000? • Registration Authority • Certificate Authority • Client (if applicable)
52.	If your current version is written for NT, will it also run on the Windows 2000 platform until the Win2000-specific version is ready? Are any special plug-ins, add-ons, or customizations needed to make this happen?
53.	Who should attend training (include Project Team, Administrators and Users (executive & non-executive)?
54.	An outline of when training needs to occur
55.	When training should be completed to avoid negative impacts on the project schedule
56.	If off-site training is available/required, please specify the geographical location(s) that training classes are offered (City, State)
57.	List other training alternatives (i.e. CD, Internet-based, CBT etc.)
58.	Does your company install the software? If yes, please provide an outline of the normal installation requirements, schedule, and acceptance criteria. Please provide a list of Installation Partners, along with contact name, and contact phone number for each.
59.	What Implementation Partners do you utilize?
60.	How is your product differentiated from your competitors?
61.	Once integration work is completed, who owns the code?
62.	If your product is not fully browser based at present, what is your strategy for offering a fully functional web-based solution?
63.	We have expended a great deal of time and effort in building our Microsoft Exchange Directory and would like to build on this. Will this be an issue? Please explain.
64.	Is the directory applicable in a distributed environment?
65.	How is 24 X 7 support handled?
66.	How many resellers/distributors does your company have worldwide?
67.	Describe the locations of your technical support centers?

RESOURCES

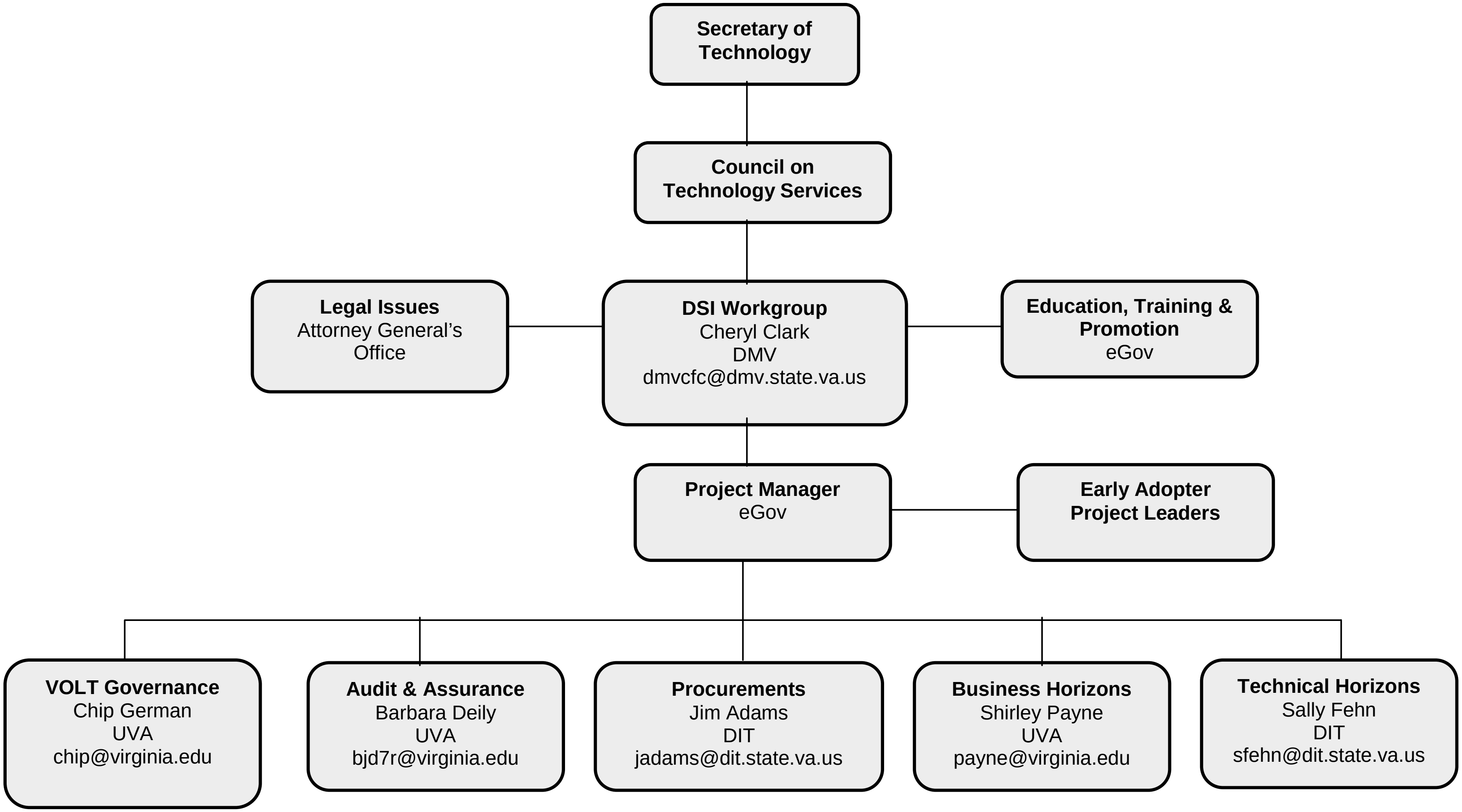
The following documents were provided to the Procurement Team:

- State of Washington RFP (Rounds 1 and 2)
- State of Utah RFP
- Aberdeen Group. "Evaluating The Cost of Ownership for Digital Certificates Projects." July 1998. http://www.directoryservice.com/WP/Aberdeen/EvalCOO.htm

APPENDIX R

PROPOSED DIGITAL SIGNATURES DEPLOYMENT WORKGROUP ORGANIZATION

October 24, 2000



Secretary of Technology

Council on Technology Services

Legal Issues
Attorney General's Office

DSI Workgroup
Cheryl Clark
DMV
dmvcfc@dmv.state.va.us

Education, Training & Promotion
eGov

Project Manager
eGov

Early Adopter Project Leaders

VOLT Governance
Chip German
UVA
chip@virginia.edu

Audit & Assurance
Barbara Deily
UVA
bjd7r@virginia.edu

Procurements
Jim Adams
DIT
jadams@dit.state.va.us

Business Horizons
Shirley Payne
UVA
payne@virginia.edu

Technical Horizons
Sally Fehn
DIT
sfehn@dit.state.va.us

- Recruit Early Adopters
- Develop CP/CPS & CONOPS
- Establish Governance
- Resolve legal, policy issues

- Advise on audit and assurance issues and standards
- Represent work group on related topics as determined

- Initiate
- Coordinate
- Administer procurements

Primary point of contact to explore, incorporate opportunities for partnership with feds, other jurisdictions and organizations

- Monitor and evaluate technical trends and issues
- Incorporate changes as appropriate

APPENDIX S

CONCEPT OF OPERATIONS OUTLINE

By Karen West, Digital Signature Trust Company
August 20, 2000

TABLE OF CONTENTS

APPENDIX S

DOCUMENT INFORMATION

PURPOSE

The purpose of this document is to define a Public Key Infrastructure (PKI) Concept of Operations (CONOP) for the Commonwealth of Virginia and its political subdivisions, including local governments. Additionally, it will describe complimentary programs to the PKI such as the Bridge CA and the statewide PIN system. It will also serve to assist in the introduction and education of the program to various participants and potential participants.

Public Key-based digital signature and encryption solutions are having a dramatic impact on security within the government and commercial market place. Numerous Commonwealth of Virginia applications are planning to incorporate this technology as part of their security solution. Based on the projected populations from some of the Commonwealth of Virginia applications, there are significant numbers of Commonwealth of Virginia users that can use this PKI within the next few years.

Cryptography has become increasingly important in the last several years. The increased use of networking (and the consequent exposure of information while transiting the network) as well as the need to protect information stored in a computer and the availability of commercial cryptographic products has fueled this increased interest. Whereas cryptography was formerly mainly a national security concern for protecting classified information, recent developments have seen greater concern for security in the commercial and government Sensitive But Unclassified (SBU) worlds. In addition, cryptographic protections for authenticity and message integrity are becoming increasingly important, whereas traditionally confidentiality was the primary concern.

Digital certificates, using cryptography, provide a superior means of authenticating oneself to a computer than traditional password protections because the latter is susceptible to guessing. An example of where this technology may be deployed is the VIPNet portal. Through this feature, each user can be authenticated via their digital certificate allowing access control for a large number of applications through one mechanism.

Digital signatures are important in electronic transactions, in that the recipient can be assured that the message really came from the person who claims to be the sender. The digital signature also provides assurance that the content has not changed since it left the sender (often referred to as data integrity), something passwords and biometrics do not provide. Integrity and authentication of documents, messages and transactions have become important within the Commonwealth of Virginia. Protection of an existing object (for example, legal document) is a key benefit of using digital signatures.

In order to successfully use cryptography, certain services such as key generation, key distribution, certificate revocation, etc., are required. A technology, known as Public Key Cryptography has developed over the past two decades, with the most dramatic advances in commercializing the technology coming in the last five years. A public key infrastructure (PKI) of sufficient size and scope to adequately address all Commonwealth of Virginia program needs within the various departments and outside the government must be deployed in order to successfully make use of the technology.

For certain applications, the use of PINs will be acceptable. [More info is needed in this section.]

A section containing a glossary of terms and acronyms can be found in Section 6 of this document.

SCOPE

The scope of this PKI covers Certification Authority services that extend to individuals, businesses, agency applications and the proposed Bridge CA. The issuance and maintenance of PINs is also covered although it is a separate system. Certificates must be used by Commonwealth of Virginia employees when conducting official public business and when a signature is required by statute, administrative rule, court rule, or a requirement of the Commonwealth. Certificates and PINs may be used to provide "evidence of authorization" in electronic business transactions where a signature is not required by statute, administrative rule, court rule or a requirement of the Commonwealth.

[Maybe some discussion here of Executive Order 65 and other initiatives that have driven the DSI.]

Included are authentication services and issuance services. Individuals and businesses that wish to receive a digital certificate in order to do business with the Commonwealth of Virginia will apply for, and be issued, a digital certificate through this program. They may also apply for and be issued a PIN.

This PKI will extend from an Intranet environment to a full Extranet environment and beyond to support e-commerce activities over the Internet. Internally, agencies will use the technology in conducting business with other internal Commonwealth of Virginia entities. In addition, commerce and business transactions will be exchanged over the Internet with external trading partners and consumers. Specifically, the following classes of transactions will need to be supported in the Commonwealth of Virginia PKI:

- Internal State Government to Internal State Government
- Internal State Government to External Government (federal, local, other States)
- Government to External Businesses
- Government to Healthcare Community
- Government to Education Community
- Government to Consumers

These same communities may also interact with local governments, participating in City and County level activities.

And finally, it's anticipated that the business community within and outside the Commonwealth of Virginia will use this technology in a business to business (B2B) exchange environment.

END ENTITIES

The PKI will serve a number of end-entities including those listed below. Internal users may be a part of the overall Commonwealth infrastructure, while others will have their own systems and infrastructure (firewalls, etc) in place. The client environment includes a variety of email clients, browser types and versions and applications.

External users will clearly have a varied environment on the desktop. Most will have compatible browsers in which to apply for certificates, others will need to download more current versions. In the case where the certificate resides in the browser, it will also be necessary to have a compatible browser. The two most popular commercial versions both support digital certificates in versions 4.0 and later. [Users will also need a 128-bit version of the browser if it's determined that keys will be 1024 in length.]

Subscribers will require a certificate carrying a level of assurance necessary to allow them access to the appropriate applications. Subscribers that require a High level of assurance must employ the appropriate level of private key storage and protection. Some users may receive PINs in order to access government services.

End entities that may participate in this PKI include:

- Government Employees (State and Local)
- Government Trading Partners (Businesses and Citizens)
- K-12 and Higher Education Community
- University Healthcare Community
- Private Healthcare Community
- Legal Community
- General Public
- Criminal Justice
- Other States, Local Governments, Federal Government

APPENDIX S

APPLICATIONS

Applications supported will include, but are not limited to:

- Browsers (Internet Explorer and Netscape Communicator)
- Email (Outlook, GroupWise, Eudora, DeVinchi)
- Software Code Signing
- Electronic Payments
- Data Files (desktop signing and encryption)
- Access Control
- Health Records
- Various G2G, G2B, G2C applications (IBM SecureWay)
- Electronic Forms

TYPES OF CERTIFICATES

Certification Authority (CA) Certificate

- Private key used by the CA to sign all end entity and server certificates

End Entity Certificates

- Individual
- Identifies an individual
- Business Representative
- Identifies an individual's affiliation with a business, agency or organization (it can also identify the individual if desired)
- Agency Applications
- Identifies an individual who is tasked with maintaining an agency application

End entity certificates may be issued to support signing, encryption, or both. That is, a single key pair and certificate can be designated for:

- Signing Only (there are technical issues here so be careful)
- Encryption Only
- Signing & Encryption

In the case of a single key pair and certificate, there is no provision for key backup and retrieval if the certificate is designated for both signing and encryption.

However, in some cases, an end-entity will generate two key pairs and be issued two certificates, one for signing and one for encryption. This will allow for the encryption key pair to be escrowed for future retrieval if supported by the Certificate Policy/rules, etc.

Server Certificates

- SSL Certificate for Web Servers to allow for SSL-encrypted sessions

APPENDIX S

CONTRIBUTORS

Contributor	Functional Team

CHANGE HISTORY

Date	Changes	Version

APPROVALS

Date	Name	Title	Signature

APPENDIX S

OVERVIEW OF BUSINESS REQUIREMENTS

ACCESS CONTROL

Certificates may be used to allow a single certificate to be presented by a Commonwealth trading partner (citizen or business), to access multiple Commonwealth data resources.

Applications that may be accessed through secure portals may include those provided by the following communities:

- State and Local Government
- Higher Education
- Healthcare

SIGNING

Certificates will be used to in support of digital signatures. Signing requirements may include, but are not limited to:

- Email (Outlook, Netscape, Eudora, GroupWise)
- Electronic Forms
- Data elements within electronic forms
- Templates
- Software code
- Permits
- Payments
- Licenses/Certificates
- Electronic files such as:
- Word documents
- Excel files

ENCRYPTION

Encryption of sensitive data files or objects may be supported, subject to the terms of the Certificate Policy. Encryption requirements may include, but are not limited to:

- Internal Government Communications, when authorized by law.
- File/Object Encryption
- Patient Identifiable Information
- Criminal Justice Information Network
- Attorney/Client Privileged Communication
- Sensitive Criminal Justice Related Information
- Desktop Encryption for protection of information.

PKI OPERATIONAL MODEL

The Commonwealth of Virginia will implement a PKI program through an out-sourced provider.   All certification authority and repository services will be provided by a Trusted Third Party who will act as the Certification Authority (CA).

The role of the Certification Authority is to provide for certificate registration, user authentication, issuance and lifecycle management of the digital certificate and/or PIN. The CA will provide for all operations pertaining to the systems that issue certificates and store them in a repository or directory. Every system maintained by the Vendor will be stored in their secure facility with failover and back-up. The registration web pages are maintained by the Vendor and all certificate requests are processed through them.   [Might want a paragraph on Agency Registration Agents (ARA/LRA) if that will be implemented.]

The Certification Authority will also host the certificate repository that holds Commonwealth of Virginia certificates and public keys. Private signature keys are generated by the Subscriber and are never in possession of the Certification Authority. All certificates issued by the Vendor follow the X.509v3 standards for digital certificates. Standards regarding Public Key Infrastructure and digital certificates can be found at the NIST web site, http://csrc.nist.gov/pki

The Vendor will issue the certificate to the appropriate browser, client software or hardware token and perform the appropriate lifecycle management of the certificate. This includes renewals, revocations and encryption key recovery.

The Vendor will assist in the creation of the Commonwealth's Certificate Policy (CP) or provide a Certificate Policy for review, which will be modeled after widely used Certificate Policies already in place including the GSA's Access Certificates for Electronic Services (ACES) Certificate Policy (http://www.gsa.gov/aces) and the US Department of Defense's CP.   ACES is a government-sponsored program designed to get certificates into the hands of the public (individuals and business) in order to interact electronically with the US federal government. The US Dept of Defense (DoD) program issues certificates to DoD's vendor community allowing them to engage in electronic commerce over the Internet in a trusted and authenticated manner.

By working toward policy interoperability, the certificates issued will be portable and accepted by a larger number of relying parties, both within and outside the Commonwealth of Virginia. This creates a higher value proposition for all PKI participants.

POLICY DOCUMENTS & ASSURANCE LEVELS

POLICY DOCUMENTS

There are three main policy documents, in addition to the CONOPS, that govern the PKI implementation. Those are the Certificate Policy, the Certificate Profile and the Certificate Practice Statement. A brief description for each is provided below.

CERTIFICATE POLICY

The Certificate Policy is a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements. Among other things, a Certificate Policy also identifies the Identification and Authentication ("I&A") processes to be performed prior to Certificate issuance, the Certificate Profile and recommended uses of the Certificate.
The Certificate Policy will be developed with the DST template as the initial document or the PMA will determine acceptable Certificate Policies for use within the Commonwealth.

CERTIFICATE PROFILE

A Certificate Profile establishes the format and content of data fields within the Certificate. Data fields within a Certificate usually identify the Issuing CA, the Subscriber, the Issuing CA's Certification Practice Statement and the operational period, and can include other information that identifies the Subscriber, such as organization, membership, licensure, etc.

The profile will also contain, among other things, the Certificate Policy OID (Object Identifier) and a unique identifier that will stay with the subscriber, not just the certificate [only leave in if you plan to use this].

CERTIFICATE PRACTICE STATEMENT

A Certificate Practice Statement (CPS) is a statement of the practices that a Certification Authority employs in issuing Certificates. The Vendor writes the CPS, outlining its adherence to the procedures set forth in the Certificate Policy.

ASSURANCE LEVELS

The Commonwealth of Virginia expects that (some number of) distinct certificate assurance levels will be supported in their PKI. Assurance levels are a function of the level of user authentication and the level of private key protection.

The matrix below outlines the assurance levels and the authentication methods and private key protection mechanisms expected to be supported.

TYPE OF CERTIFICATE	HIGH ASSURANCE	MEDIUM ASSURANCE	PIN
Authentication			
In Person - Notary	X	X	Not Required
ARA/LRA – State Agency to include third party cross check against databases	X	X	Not Required, but not precluded
Online – thru DST	Not Acceptable	X	X
Private Key Protection			
Cryptographic Hardware or Software Module	X	Not required	N/A
Browser Only	Not Acceptable	X	N/A

As such, each Subscriber must be educated to understand the assurance level/tool most appropriate for their needs. Applicant identification & authentication (I&A) procedures and private key protection methods will be defined in greater detail in the Commonwealth of Virginia Certificate Policy or list of approved Certificate Policies.

PKI AND OTHER SERVICES TO BE PROVIDED

REGISTRATION AND AUTHENTICATION

Registration will be dependent on the type of certificate that is issued and will be further defined in the appropriate Certificate Policy(s). It is generally accepted that a single level of assurance will not suffice for all applications.

At the time of the publication of this CONOPS document, 2? assurance levels have been defined; High and Intermediate.

The three types of registration supported by DST are:

- In Person Presentment to an Approved Notary
- Vendor will also perform a background check on the information submitted
- Out of band delivery of activation code
- Local Registration Agent Authentication within the Government sector
- Vendor will also perform a background check on the information submitted
- Out of band delivery of activation code
- Online Application through Vendor
- Vendor will perform a background check on the information submitted
- Out of band delivery of activation code

The chosen vendor will provide several kinds of authentication services for Subscribers, depending on the requirements of the Certificate Policy. It is anticipated that these services will include most, if not all of the following:

In-Person Application

- Applicant submits identity information to DST through web site using an SSL encrypted session to ensure confidentiality during transmission
- Applicant also prints out information, has it notarized and mails to DST
- DST performs I&A on applicant and notary
- DST sends an out of band (US Mail) notification with activation codes
- Applicant returns to DST and retrieves their certificate

Local or Agency Registration Agent

- Once the ARA/LRA has been authenticated by the Vendor, that person will perform the registration duties for individuals within their agency/public entity
- The ARA/LRA will also have the authorization to request renewals, revocations and encryption key recoveries on behalf of their agency/public entity

Online Application

- Applicant submits identity information to the vendor
- Vendor performs I&A on applicant
- Vendor sends an out of band (US Mail) notification with activation codes
- Applicant returns to Vendor site and retrieves their certificate

CERTIFICATE MANAGEMENT

The Vendor will provide full certificate lifecycle management. The Certificate Enrollment and Issuance process is defined in greater detail in the Commonwealth of Virginia Certificate Policy(s). Certificate management services will include, but are not necessarily limited to:

CERTIFICATE PUBLISHING

All certificates are published to an LDAP directory once retrieved by the Subscriber. DST maintains a master read/write directory behind all firewalls, not allowing public access. The information, including the CRL, is then replicated to a public directory outside the firewall.

CERTIFICATE RENEWAL

Certificate renewal may be automatic or manual. In the case of automatic renewal, client software can initiate the renewal and key rollover process without additional user intervention.

In the case where client software is not present to perform this task, the Subscriber will be notified via email before certificate expiry and given instruction on how to renew their certificate(s).

CERTIFICATE REVOCATION

DST verifies all revocation requests before any revocation is performed. A Subscriber may request a revocation of their own certificate, an ARA/LRA may request the revocation of a certificate they approved or DST may determine that a private key has been compromised and revoke a certificate. In all cases, DST notifies the Subscriber of the revocation.

CERTIFICATE KEY UPDATE

Keys are updated at the time of certificate renewal.

CERTIFICATE VALIDATION

All certificates are created with the Certificate Distribution Point (CDP) published within the certificate. The CDP contains the location of the directory and CRL where the certificate can be validated.

CRL PUBLISHING

Certificate Revocation Lists are published no less than once every 24 hours. The CRL can also be pushed to a local directory to facilitate the validation process for internal use.

ON-LINE CERTIFICATE STATUS CHECKING

The Online Certificate Status Protocol (OCSP) may be supported by applications for which web/browser based certificates are used. The application would only need an OCSP responder; the Vendor must have the ability to support OCSP in their directory services.

CRYPTOGRAPHIC TOKEN MANAGEMENT

SOFTWARE TOKENS

End-user client software may be available to store and protect the private key and certificate. Private keys can be generated in the client software and are portable to any machine onto which the client software has been loaded. [This would apply if Entrust were used or some third party software such as E Lock. Otherwise, the private key resides in the browser.]

HARDWARE TOKENS

End-user hardware tokens are available to store and protect the private key and certificate. Private keys can be generated onto the hardware token and portable to any machine that contains the appropriate reader or token interface (e.g. USB port.) Once generated on the token, it is not possible to export that private key.

DIRECTORY/REPOSITORY SERVICES

DIRECTORY ACCESS

DST maintains a master read/write directory that resides behind all firewalls. DST may publish or mirror this information to a directory that is read only and accessible to outside entities for purposes of validation. It is also possible to have the CRL pushed to a local site for purposes of validation.

DIRECTORY SCHEMA

Vendor will provide customer agencies with its directory schema that will allow copies of certificates and CRLs to be posted locally.

DIRECTORY MANAGEMENT AND MODIFICATION

DST will manage and modify its read/write directory housed onsite at the Vendor's secure facility. Vendor will also publish the CRL and other information to local directories housed at the Commonwealth of Virginia if requested by agencies.

OTHER SERVICES

KEY ESCROW AND RECOVERY

The Vendor may be required to escrow the private decryption key for Subscribers to help prevent the loss of valuable information and documents. Private signature keys are never escrowed at any time. The end-entity or

Encryption key recovery is supported only when dual key pairs and certificates are issued, one for signing and one for encryption.
[Even if you decide to exclude encryption from requirements leaving it in the CONOPS gives you flexibility down the road]

TIME-STAMPING

Time stamping services are provided for all validation activity within the Vendor repository. Additional timestamp services are available to provide complete audit trails for each leg of a transaction.

SUPPORT AND HELP DESK SERVICES

DST will provide the following types of support for subscribers and local registration agents: [this is fairly specific to DST, you'd want to determine your helpdesk requirements]

Web Site

- Frequently Asked Questions (FAQ)

HelpDesk

Online

- This service is offered on a 24 x 7 basis

Email

- This service is offered on a 24 x 7 basis

Phone

- Support hours are 6am-6pm MT

Training

- Certificates (and PINs?) will be issued to a select group of agencies and trading partners, who will participate in the CA and PKI Services "Early Adopter Program". This pre-production activity will test the registration, issuance, and installation of any software or hardware modules and applications.
- Vendor will be on-site for installation of software and certificate registration to assist the participants in those activities. As the program proceeds, the Vendor will hold regular on-site training and informational sessions.

ACRONYMS & GLOSSARY OF TERMS

ACRONYMS

ARA	Agency Registration Agent
B2B	Business to Business
B2C	Business to Consumer
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
DST	Digital Signature Trust Co.
I&A	Identification & Authentication

G2B	Government to Business
G2C	Government to Consumer
G2G	Government to Government
FIPS	Federal Information Processing Standard
LDAP	Light-weight Directory Access Protocol
LRA	Local Registration Authority
NIST	National Institute of Standards & Technology
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adelman; a proprietary asymmetric cryptographic algorithm
SHA	Secure Hash Algorithm
USB	Universal Serial Bus
VIPNet	Virginia Information Providers Network

GLOSSARY OF TERMS

TERM	DEFINITION
Access Control	The process of ensuring that systems are accessed only by those authorized to do so, and only in a manner for which they have been authorized.
Algorithm	An algorithm is a set of rules that specifies a method of carrying out a task (e.g., encryption algorithm).
Archive	To store records and associated journals for a given period of time for security, backup, or auditing purposes.
Audit logs	All significant transactions that are recorded in audit logs. Audit logs are valuable because they record all significant operations.
Authentication	The process of assuring that data has come from its claimed source, or of corroborating the claimed identity of a communicating party. Certificates are used to identify the author of a message or entity, such as a Web server or client. People or applications that receive a certificate can verify the identity of the certificate's owner and the validity of the certificate. This process is known as authentication.
Authorization	Determining whether a subject is trusted for a given purpose.
Backup	A copy of computer data that is used to recreate data that has been lost, mislaid, corrupted, or erased.
Browser	A client program that is used to look at various kinds of Internet resources.
Certification Authority (CA)	An entity that issues and manages certificates within a PKI.
CA certificate	A certificate that identifies a CA. When a CA issues a certificate to a client, a server, or other entity, the certificate is signed by the CA's private key. The signature can be verified using the public key in the CA's certificate.

TERM	DEFINITION
Certificate	A digital identifier linking an entity and a trusted third party able to confirm the entity's identity. It is used to verify the identity of an individual, organization, or Web server, and to ensure non-repudiation in business transactions. Three major kinds of certificates are used in a PKI: CA certificates, server certificates, and end-entity certificates.
Certificate Revocation List (CRL)	An enumeration of certificates that have been revoked by a particular CA. CRLs can be used to check the status of certificates offline.
Certificate Serial Number	A value that unambiguously identifies a certificate generated by a CA.
Certification Authority (CA)	A trusted entity issuing certificates and confirming the identity of, or given facts about, the certificate's subject.
Client (servers)	A machine that retrieves information from a server.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. (See Data Integrity) The loss of a key through noncryptanalytic means.
Confidentiality	The process of ensuring that data is not disclosed to those not authorized to see it. Also known as secrecy.
Cryptography	The art or science of transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key.
Customer	The customer is any person authorized by a data owner to read, enter, or update that person's data.
Data Integrity	Measures to prevent unauthorized alteration of data, deciphering, or conversion of ciphertext back into plaintext.
Database	A set of related information created, stored, or manipulated by a computerized management information system.
Decrypt	To decrypt a protected file is to restore it to its original, unprotected state.
Decryption	Decryption is the process of transforming ciphertext back into plaintext. It is the reverse of encryption.
Digital Signature	A data element allowing the recipient of a message or transaction to verify the content and sender.
Directory	Databases that can be used to search for and retrieve attribute-value pairs. Directories can be configured to use (or support) authentication and access control protection. The schema of a directory describes the objects in the directory.
DST	Digital Signature Trust Co. Also refers to computing resources and computer-related facilities specifically assigned by Digital Signature Trust Co. to DST for operations and maintenance.
Encrypt	To encrypt a file is to render the file completely unreadable. No one can read the file until it is decrypted. Only authorized recipients can decrypt the file. You (the key owner) have full control in determining authorized recipients.
Encryption	A process of disguising information so that an unauthorized person cannot understand it.
End-entity certificate	A certificate issued to an entity that cannot itself issue certificates (in essence, it is not a CA). Because the entity that requests such a certificate is sometimes referred to as the client, end-entity certificates are sometimes called client certificates.

TERM	DEFINITION
Entity	A person, computer, organization, or piece of information. In a PKI, an entity may be thought of as anything to which a certificate may be issued.
Firewall	A combination of hardware and software that separates a LAN into two or more parts for security purposes.
Frequently Asked Questions (FAQ)	FAQs are documents that list and answer the most common questions on a particular subject.
Generate a Key Pair	A trustworthy process of creating private keys whose corresponding public keys are submitted to the applicable IA during certificate application in a manner that demonstrates the applicant's capacity to use the private key.
Identification and Authentication (I&A)	A process that identifies and authenticates a person or a business that applied to receive a digital certificate.
Identity certificate	A certificate that links a public key value to a real world entity such as a person, a computer, or a Web server. Server certificates, CA certificates, and most end-entity certificates are all examples of identity certificates.
Integrity	The element of data protection concerned with ensuring that data cannot be deleted, modified, duplicated, or forged without detection.
Internet	A global public network consisting of millions of interconnected computers all linked together using the Internet protocol.
Issuing	The act of signing a certificate request with the private key of a CA to create a certificate.
Key	A special number that an encryption algorithm uses to change data, making that data secure.
Key lifetime	The length of time for which a key is valid. All keys have a specific lifetime except the decryption private key, which never expires. Default key lifetimes are defined by Security Officers as part of an organization's security policy.
Key management	Administering keys securely so that they are provided to users where and when they are needed. Processes associated with the secure generation, transport, storage, and destruction of encryption keys.
Key recovery	A key management process associated with the retrieval of a key lost by the key holder to ensure access to ciphertext created with the key in question.
Key update	When key pairs are updated, they are replaced with the new key pairs, and new public key certificates are created. The new keys and certificates have no relation to the old keys and certificates.
Key	When used in the context of encryption, a series of numbers which are used by an encryption algorithm to transform plaintext data into encrypted (ciphertext) data, and vice versa.
Lightweight Directory Access Protocol (LDAP)	The standard Internet protocol for accessing directory systems over a network. LDAP is a "lightweight" (smaller amount of overhead) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network. Sentry's Secure Directory is an LDAP directory.
Lightweight Directory Applications Protocol	The Internet standard for simple directories for use in messaging and similar applications.

TERM	DEFINITION
National Institute of Standards & Technology (NIST)	The National Institute of Standards and Technology (NIST) is taking a leadership role in the development of a Federal Public Key Infrastructure that supports digital signatures and other public key-enabled security services. NIST is coordinating with industry and technical groups developing PKI technology to foster interoperability of PKI products and projects.
Netscape Communicator	A Web browser, widely recognized and popular.
Out-of-band	Not in the electronic pipeline; any communication which is not computer-to-computer such as US Mail.
Password	A sequence of characters that allows users access to a system. Although they are supposed to be unique, experience has shown that most people's choices are highly insecure. People tend to choose short words such as names, which are easy to guess.
Personal Identification Number (PIN)	A sequence of digits used to verify one's identity for access to applications. It can also be used as a sequence of digits used to verify the identity of the holder of a token. It is a type of password.
Policy	An informal, generally natural language description of desired system behavior. Policies may be defined for particular requirements, such as confidentiality, integrity, availability, safety, etc.
Portal	The place people see when using the Web. It can be a front door to a variety of services and applications and is generally the starting point for users of those services and applications.
Private Key	The private part of a key pair. Private keys are generated on the client in most cases. Private keys must be securely stored to prevent unauthorized access and accidental deletion. In general, information encrypted with a private key can only be decrypted with the corresponding public key. A digital signature signs messages with a private key and allows anyone with a corresponding public key to read the message to be certain of who sent the message and ensure that it has not been tampered with.
Protocol	A series of steps involving two or more parties designed to accomplish a task.
Public Key	The public and widely distributed part of a key pair. A cryptographic key employed in public key cryptography to encrypt (usually small) amounts of data to the key's owner, or to verify the key owner's signature. A certificate contains information about the certificate subject, the certificate's signer, and a public key value. In general, information encrypted with a public key can only be decrypted with the corresponding private key. It can be published without revealing the owner's corresponding private key.
Public key algorithm	An asymmetric algorithm, so designed that the key used for encryption is different from the key used for decryption.
Public Key Cryptography	A form of asymmetric encryption where all parties possess a pair of keys, one private and one public, for use in encryption and digital signing of data.

TERM	DEFINITION
Public Key Cryptography Standard (PKCS)	A set of commonly applied data cryptography standards developed by RSA Data Security Inc. for making secure information exchange possible. The standards include RSA encryption, password-based encryption, extended certificate syntax, and cryptographic message syntax for S/MIME, RSA's proposed standard for secure e-mail.
Public Key Infrastructure (PKI)	A system for publishing the public key values used in public key cryptography. Also a system used in verifying, enrolling, and certifying users of a security application. All PKIs involve issuing public key certificates to individuals, organizations, and other entities and verifying that these certificates are indeed valid.
Recovering a user	Recovering means generating a new signing key pair and securely retrieving from the Certification Authority, your current encryption public key certificate, decryption private key history, verification public key certificate, and CA verification public key certificate.
Registration Authority (RA)	The part of a PKI involved in verifying and enrolling users. RAs work with a particular CA to vet requests for certificates that will then be issued by the CA.
Repository	A database of certificates and other relevant information accessible online.
Repudiation	The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.
Revocation	Revoking a certificate makes the certificate invalid, effectively suspending all of the certificate user's privileges in the PKI. Revocation is necessary if the CA administrator wants to retract the certificate before it expires. Certificates are revoked by marking them as invalid in the Secure Directory. Users of the PKI are notified of a certificate's revoked status during online validation or with CRLs.
Root	The IA that issues the first certificate in a certification chain. The root's public key must be known in advance by a certificate issuer in order to validate a certification chain. The root's public key is made trustworthy by some mechanism other than a certificate, such as by secure physical distribution.
Root CA	The source CA is a certification path. Generally, the Root CA is a self-signed CA that is used to sign the certificates of other CAs. The Root CA may also be referred to as a top-level CA to reflect the CA's position in a hierarchical PKI.
RSA keys	The encryption keys employed in the RSA cryptography system.
Schema	A schema describes an object and its attributes in LDAP.
Secure Sockets Layer (SSL)	An encryption standard devised by Netscape Communications for secure communication over the World Wide Web. SSL is a protocol layer created by Netscape to manage the security of message transmissions in a network. The "sockets" part of the term refers to the sockets method of passing data back and forth between client and server programs in a network or between program layers in the same computer. Now in widespread use in all Web browsers. It is about to be superseded by TLS, an open standard developed by the IETF.
Secure/Multipurpose Internet Mail Extensions (S/MIME)	S/MIME is a specification for secure electronic mail and was designed to add security to e-mail messages in MIME format. The security services offered are authentication (using digital signatures) and privacy (using encryption).

TERM	DEFINITION
Security	The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific “state” to be preserved under various operations.
Server	A machine running a service. A Web server provides a Web-based information service to a community of machines. A computer, or a software package, that provides a specific kind of service to *client* software running on other computers.
Server Certificate	A certificate issued to a server. Servers present their certificates to Web browsers so they can verify (authenticate) the identity of the server. Server certificates are sometimes called SSL certificates.
SHA-1	Secure Hash Algorithm—a hash function first originated by the US National Security Agency and National Institute of Standards and Technology.
Signer	A person who creates a digital signature for a message or a signature for a document.
Smart Card	A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering. A plastic card (looks like a credit card) with an embedded computer chip, used most widely in Europe. Many countries use the smart card for pay telephones. There are also smart credit cards and smart cash cards.
SSL Server Authentication	The process whereby a client application authenticates a server by verifying the certificate chain presented by the server during SSL operations.
Subscriber Agreement	The agreement executed between a subscriber and a CA for the provision of designated public certification services in accordance with this CPS.
Test Certificate	A certificate issued by a CA for the limited purpose of internal technical testing. Test certificates may be used by authorized persons only.
Time Stamp	A notion that indicates (at least) the correct date and time of an action and the identity of the person or device that sent or received the time stamp.
Token	A physical object, often containing sophisticated electronics, which is required to gain access to a system. Some tokens contain a microprocessor, and are called intelligent tokens, or smart cards.
Trust	A person or system in which confidence or faith is placed.
Trusted Third Party (Schneier)	An agency providing security related services and activities to one or more entities in a given security infrastructure.
Type of Certificate	The defining properties of a certificate, which limit its intended purpose to a class of applications uniquely associated with that type.
Uniform Resource Locator (URL)	A URL is used to specify the location and name of a World Wide Web document, for example, http://www.digsigtrust.com . Previously called *Universal Resource Locator*.
Universal Resource Locator (URL)	Same as *Uniform Resource Locator*.
User	Any person utilizing resources provided and maintained by Digital Signature Trust Co. (DST). An authorized entity that uses a certificate.

TERM	DEFINITION
User authentication	Determining that a user truly is authentic.
Validation	The process of verifying that a certificate is still valid. Validation can occur online or through the use of CRLs.
VIPNet	Commonwealth of Virginia application portal that provides an authentication gateway and single sign-on for applications state and local government agencies choose to register. Trading partners will be allowed access to certain applications through a credential such as a digital certificate. Some applications will require a specific assurance level of certificate in order to be accessed or a PIN. Others will not require anything to be accessed.
World Wide Web	The whole constellation of resources that can be accessed using *Gopher, FTP, HTTP, telnet, USENET, WAIS* and some other tools. A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium. A collection of linked documents that reside on the Internet.
X.509	The ITU (International Telecommunications Union) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions. Also an International Standards Organization (ISO) standard that describes a basic electronic format for digital certificates.
X.509 v3 Certificate Extension	The PKI suites used by DST support X.509 v3 certificate extensions including extensions for PKIX, SET, and SSL. These extensions conform to the X.509 standard and specify additional constraints or capabilities on the certificate subject.

SCHEDULE

Major milestones are listed below:

First Draft	Date 2000
Meeting to Discuss Draft #1	Date 2000
Complete Draft #2	Date 2000
Review	Date 2000
Final Review	Date 2000
Finalize CONOPS	Date 2000

APPENDIX T

VOLT EARLY ADOPTERS PROGRAM CONCEPT PAPER

By Sally Fehn, Department of Information Technology
September 7, 2000

BACKGROUND: WASHINGTON STATE LESSONS LEARNED

Karen West, a consultant with Digital Signature Trust Corporation (DST), provided the Digital Signature Initiative Workgroup with lessons learned from the Washington State PKI deployment. DST won the state of Washington contract to provide the statewide PKI infrastructure and services. After deliberation over many issues, the current direction in the Washington contract is to bring up select applications under the PKI infrastructure in what they are calling the “early adopter” projects. The selected applications will be presented as models for future deployment of PKI in the state. Additionally, it is hoped that the applications will be well accepted and provide winning strategies for bringing customers onboard.

USING THE EARLY ADOPTER MODEL FOR THE COMMONWEALTH OF VIRGINIA

The DSI workgroup is proposing a similar approach as Washington by identifying applications to use as “early adopters” of Public Key Infrastructure (PKI). The DSI workgroup is seeking assistance from the Electronic Government Implementation Division (EGID), as directed in ***Executive Order 65(00),*** to provide funding support for this initiative and coordination of resources between the agencies, institutions of higher learning and local governments. The concepts identified in this paper are for consideration for incorporation into the RFP for a statewide PKI, associated services, and application integration solutions. The Department of Information Technology (DIT) will manage the contracts awarded as a result of the RFP, including Certificate Authority services, integration services, and application reengineering services.

The Early Adopters applications will be large-scale prototypes implemented in a production environment. The stable, operational environment will provide for controlled modifications and refinement of the technology. Applications that can be logically enabled to incorporate certificate cross-certification or use an interoperability mechanism between certificates issued by more than one vendor is a key infrastructure component. The outcome of the initiative will be a solid infrastructure that will support the use of digital signatures for electronic government applications in the Commonwealth of Virginia.

CONCEPTS FOR THE EARLY ADOPTERS PROJECTS

State Portal Strategy. By providing integration and directory services, configure the Commonwealth of Virginia homepage to provide a seamless look between agencies; eliminating stovepipe, agency centric approach to services. DIT would provide access control services and integrated directory services for the state portal to achieve a customer- focused approach to state agency and locality websites. Eventually, a single sign-on mechanism could be employed to build customer tailored portals.

Develop Customer Satisfaction Metrics. When developing the applications, plan ahead to gather statistical information from the user:

- Build automated features into the applications to gather data about the user population and usage
- Provide electronic surveys to get feedback

Partnerships Of Agencies and Local Governments. Change approach of PKI development projects in local and state government to provide services that cross agency boundaries and are:

- Customer focused
- Self service, interactive, provide information and transactions
- Have extended hours, possibly 24 hours, 7 days a week
- Easily accessible and speedy
- Could eventually provide a value add feature (a citizen logs on to look at information and a reminder appears that their driver’s license needs to be renewed this year and the book they ordered at the library is in)

Partnerships With Vendors. Collaborate with vendors to have them help provide vision and interoperable technology across agencies by:

- Leveraging technical knowledge and tools across agencies
- Providing a platform to strengthen the ability and lessen the timeframe for each agency to bring applications up on the Internet

Coordinate With Other Virginia Electronic Government Workgroups. Participate and coordinate with other Virginia Electronic Government Workgroups to bring a cohesive infrastructure to the Commonwealth's Internet presence and eliminate duplicate effort.

Work with the Electronic Government Implementation Division to incorporate the implementation of directives in ***Executive Order 65 (00)*** in the Early Adopter Initiative:

- Develop the policies, standards, and guidelines necessary for statewide deployment of digital signatures
- Facilitate the procurement activities relating to statewide deployment of digital signature technology
- Develop educational programs on how to implement secure digital signature technology
- Ensure that the implementation of digital signature technology by the Commonwealth complies with UETA
- Identify changes necessary to implement Web-based systems that can be directed through policy directive, Executive Order, change in regulation, or amendment of the *Code of Virginia.*

Additionally, incorporate the findings of the Digital Opportunity Task Force, as established in ***Executive Order 65 (00),*** into the Early Adopter project to:

- Find ways to expand public access to computers and the Internet through community-based resources
- Help to establish a clearinghouse of best practices and resources to allow replication of the ideas

Work With eGov To Integrate Resources.

Identify core business functions that are candidates for cross agency deployment:

- Eventually standardize and push data across agencies, i.e., changes in name, address, and phone number
- Purchase in volume to get greater vendor discounts
- The possibility exists to provide free certificates to users or allow usage of a Federal ACES certificate
- Identify, develop, and reuse modules across agencies, i.e., electronic payment, data access control, digital certificates, data warehouse

DISCRIMINATORS TO FIND CANDIDATE APPLICATIONS

Use the Digital Signatures Decision Model developed by the Audit Group to find current processes/applications that meet the requirements for digital signatures and possess some of the following traits and encompass G2G, G2B, and G2C transactions:

- Require manual signatures as a step in the process
- Current process is cumbersome, manual intensive
- The flow of the application causes a delay in processing
- Requires physical presence to complete an identification process
- Applications that are under the jurisdiction of Secretary Upson
- PKI could replace PIN authentication across multiple applications (single sign-on)
- Are recurring processes for users
- Have documents that must be faxed in, and then require a response
- For initial deployment, the process has a lower limit of liability or lower risk if a digital certificate is compromised

ADMINISTRATIVE APPLICATIONS IN EO65

Other applications that are candidates for the Early Adopter project are identified in EO65 as a “wide range of administrative processes within state government that could be web-enabled to help government operate more efficiently”. These processes are used by virtually every agency in the Commonwealth and include but are not limited to:

- Employee benefits administration
- Leave reporting and accounting
- Travel planning and booking
- Travel Reimbursement
- Motor pool reservations
- Expense reporting

The plan for developing web-based versions of these processes is to be submitted to the Secretary of Technology by the end of October 2000.

ISSUES FOR RESOLUTION

Additional issues that need resolution to provide a framework for deploying Early Adopter applications:

- Does existing legislation require any changes to allow the use of a digital signature, i.e., current state statute requires a manual signature?
- Is additional legislation needed to provide the mandate for inter-agency cooperation, participation, development and funding under the leadership of EGID?
- What is the role of VIPNet in developing a state portal and assisting agencies with web deployment? Are there already plans for the state portal to provide a seamless look across agencies? Is there a five or ten year plan for the state website?
- Contrary to most site security policies, most users are not familiar with and are not using procedures to secure their PC. Only a culture change would bring it about, and that is unlikely. For that reason, maintaining a certificate in a browser on a PC does not have a high degree of security. In addition, many users change PCs or have other co-workers accessing their PCs for various reasons. An application that requires the degree of authentication that PKI supports implies that the certificate must be secure. Smart cards, tokens, and biometrics are better candidates for maintaining secure authentication and for giving the user mobility.
- What are the limits of liability for each participant in a PKI environment? Trained legal personnel should examine and help construct the certificate policies and practice statement. What does the CA assume liability for in terms of dollar limits? Is this a possible reason to require an outsourced CA?

EARLY ADOPTERS INITIATIVE—COST CONSIDERATIONS

The major cost considerations to build the infrastructure for the Early Adopters Initiative are identified below.

Initial investment:

- Establish a reserve fund controlled by SOTECH, to provide the funding for the Early Adopters projects to develop digital signature applications. Current agency budget request constraints and length of time until the next budget cycle prohibits quickly moving forward on this initiative in this calendar year.
- Identify applications and document the requirements for Early Adopters projects using funding from the reserve.
- Develop a Central Contract to acquire the services of a technology and vendor neutral PKI Integrator. The integrator would assess the application requirements, and then provide the infrastructure solution of products and services.

If an **in-house Certificate Authority** model is deployed, the Infrastructure Cost Model must consider all of the following items:

- Policy Documents Development
- Policy Statement
- Certificate Practice Statement
- Registration Policy
- Subscriber Agreement

PKI Staff (Depends on how many users, RA's, are being serviced.)

- Policy Authority
- Operations Authority
- PKI Manager
- Auditing

DESIGN AND INTEGRATION

- Product Evaluation
- Infrastructure Integration

FACILITIES

- Secure CA Facility
- Certificate Authority, primary CA server
- CA software license
- Enterprise Directory
- Directory license
- Firewall hardware
- Firewall software

LICENSING

- PKI User Certificate
- LDAP Directory Entry

CERTIFICATE MANAGEMENT STAFF

- Issue User Certificate
- Recover Certificates
- Directory Distinguished Name Change
- Revoke Certificate

Cost factors. To establish a basis for cost, an estimate of the total number of users must be provided. As the number of users increases, the cost per user decreases. As a side note, the number of certificates issued is usually not a factor, only the number of users. One user can have multiple certificates with different assurance levels. Therefore, the total cost model must be developed showing costing levels with increasing numbers of users.

APPENDIX U

PROPOSED VOLT GOVERNANCE CHARTER

By Chip German, University of Virginia
August 28, 2000

(Adapted from the Federal Public Key Infrastructure Policy Authority documents)

1. Definitions

1.1. Agency, Institution of Higher Education, Local Government, Entity

1.1.1. "Agency" shall mean any state agency as defined in [insert Code of Virginia citation here]. It shall not include subordinate elements within an agency.

1.1.2. "Institution of Higher Education" shall mean any state institution of higher education as defined in [insert Code of Virginia citation here]. It shall not include subordinate elements within an institution of higher education.

1.1.3. "Local Government" shall mean any government [insert appropriate citation here]. It shall not include subordinate elements of a local government in Virginia.

1.1.4. "Entity" shall mean any organization described in Definition 1.

1.2. "Voting member" shall mean any person who has been appointed to membership of the VOLT Standards Committee by the Secretary of Technology.

2. Purpose and Other General Information

2.1. Purpose. The VOLT Standards Committee, a body of the Commonwealth of Virginia's Council on Technology Services, sets policy governing operation of the Commonwealth of Virginia implementation of public key infrastructure generally and the particular functions represented by its two primary functional components, the Commonwealth of Virginia Central PKI Service and the Commonwealth of Virginia Bridge Certification Service. The VOLT Standards Committee is created under the authority of the Secretary of Technology pursuant to Code of Virginia § 2.1-51.47 B3(ii) and Governor James Gilmore's Executive Orders 51, 65 and 66.

2.2. Scope of Responsibilities. Determinations by the VOLT Standards Committee apply to the issuance of certificates by the Virginia Central PKI Services vendor and the Virginia Bridge Certification Service to state entities but do not prescribe how those entities are to rely on certificates in general for transactions; entities are free to accept or reject certificates issued by other governmental or non-governmental organizations at their discretion, using VOLT Standards Committee determinations to assist in making informed decisions.

2.3. Caveat. The VOLT Standards Committee makes no guarantees against fraud or loss resulting from its activities.

3. Roles and Responsibilities of the VOLT Standards Committee

3.1. Develop a concept of operations document for the VOLT-related PKI environment that can serve as the basis for RFPs that seek (1) a vendor to provide central PKI services for the Commonwealth and (2) a vendor or set of vendors who can assist agencies in making applications VOLT PKI-ready.

3.2. Develop and adopt VOLT certification policy and practice statements, operating rules, and applications processes with appropriate advice from involved parties.

3.3. Coordinate review and resolution of legal, policy, technical, and business issues related to state entity use of PKI certificates and their interoperability

3.4. Roles and Responsibilities of the VOLT Standards Committee with respect to the Virginia Bridge Certification Service (to be executed when appropriate)

3.4.1. Enter into an agreement with the Virginia Bridge Certification Service which establishes that: (a) the Virginia Bridge Certification Service will effect or terminate interoperation with Commonwealth of Virginia entities only when directed by the VOLT Standards Committee and (b) the VOLT Standards Committee may review Virginia Bridge Certification Service activities for compliance with the Bridge Certification policies and practices set by the committee.

3.4.2. Perform liaison efforts with external parties, including companies, other governments within the U.S. (federal, state, and local), and foreign governments. The VOLT Standards Committee covers only Commonwealth of Virginia entities, and the Virginia Bridge Certification Service initially will support interoperation among state entity PKIs and interoperation among those entity PKIs and those of federal agencies; ultimately, interoperation through the Virginia Bridge Certification Service may be extended to parties external to those entities, when and how the VOLT Standards Committee deems appropriate.

3.5. Roles and Responsibilities of the VOLT Standards Committee with respect to the Virginia Central PKI Services vendor

3.5.1. Enter into an agreement with the Virginia Central PKI Services vendor which establishes that: (a) the Virginia Central PKI Services vendor will operate under the policies and practices set by VOLT Standards Committee and (b) the VOLT Standards Committee may review Virginia Center PKI Services vendor's activities for compliance with policies and practices set by the committee.

3.6. Roles and Responsibilities of the VOLT Standards Committee with respect to user groups

3.6.1. The VOLT Standards Committee will make formal provision in its meetings to receive input from representatives of groups comprising VOLT certificate users and PKI bridge users, subject to reasonable limitations on means and duration of presentations.

3.6.2. The Secretary of Technology or his or her designee shall assist communication among users of VOLT certificates and among users of the PKI Bridge by establishing list-servs or similar mechanisms to promote open discussion of issues.

4. Membership and Organization

4.1. Membership in the VOLT Standards Committee

4.1.1. Voting members are appointed by the Secretary of Technology. A voting member may be removed by the Secretary of Technology for excessive absences or other failures to participate in the activities of the VOLT Standards Committee.

4.1.2. The terms of voting members shall be two years from the date of their appointments, and they may be re-appointed without limitation on number of successive terms.

4.2. The VOLT Standards Committee primary structure

4.2.1. The Virginia Central PKI Services function

4.2.1.1. The Virginia Central PKI Services component includes three elements:

4.2.1.1.1. The VOLT Standards Committee's direct activities related to the Virginia Central PKI Services function;

4.2.1.1.2. The VOLT Standards Committee's Central PKI Services subcommittee, which drafts certificate policy and operating rules, outlines the certificate granting process, reviews violations of policy and practices by agencies, and may recommend revoking certificates; and

4.2.1.1.3. The Virginia Central PKI Services vendor, which issues certificates and performs related services under the oversight of the VOLT Standards Committee and its Central PKI Services subcommittee.

4.2.1.2. The function of the Virginia Central PKI Services is to provide an opportunity for Commonwealth of Virginia entities to use a standard certificate mechanism without having to operate or contract for their own certificate authorities.

4.2.2. The Virginia Bridge Certification Service

4.2.2.1. The Virginia Bridge Certification Service component includes three elements:

4.2.2.1.1. The VOLT Standards Committee's direct activities related to the Virginia Bridge Certification Service;

4.2.2.1.2. The VOLT Standards Committee's Bridge subcommittee, which drafts policy and practice statements, operating rules and applications processes, considers applications to participate, negotiates trust mapping, and reviews violations of agreements by entities and may recommend removal of participant status of such entities; and

4.2.2.1.3. The Virginia Bridge Certification Service, which cross-certifies agency certificates via the bridge and performs related services under the oversight of the VOLT Standards Committee and its Bridge subcommittee.

4.2.2.2. The Virginia Bridge Certification Service's purpose is to provide one means by which Commonwealth of Virginia entities that are employing public key technology to interoperate efficiently when they operate their own certificate authority or when they use certificates issued by other certificate authorities. Through processes developed by the Bridge Certification Service, an entity's public key infrastructure can be allowed to trust digital certificates issued by other entity PKIs. Use of the Bridge Certification Service is not mandatory; entities may accomplish interoperability of their PKIs by other means if they so choose.

4.3. Other structures related to The VOLT Standards Committee. The VOLT Standards Committee may have other subcommittees or working groups as determined by majority vote of the voting membership, to support its operation. Membership on those subordinate committees or working groups shall also be determined by majority vote of the voting membership and generally shall not be limited to members of the VOLT Standards Committee.

5. Officers

5.1. The VOLT Standards Committee shall have a Chair and a Vice Chair, both selected by majority vote of the voting membership. The Chair shall serve a two-year term. The first Vice Chair shall serve a one-year term, and subsequent Vice Chairs shall serve two-year terms, thus providing overlap with the term of the Chair.

5.2. The VOLT Standards Committee shall have a Secretary appointed by the Secretary of Technology who shall record minutes of all VOLT Standards Committee meetings, including recording a listing of all persons present at meetings and who they represent, and be responsible for administrative matters.

6. Operation

6.1. Meetings shall be held on a schedule to be determined by majority vote of the voting membership. The Chair or, in his or her absence, the Vice Chair, shall preside. All members will be given reasonable notification before any vote is called, all votes shall be recorded, and the results of voting will be published.

6.2. For actions requiring votes, the voting may be done at a VOLT Standards Committee meeting, through remote means, or by proxy granted by the voting member to another voting member or to an alternate designated by the member and identified to the Chair in advance of the vote. Each voting member shall be required to cast a vote, except when recusal is necessary owing to a conflict of interest. Failure of a voting member to vote during the voting period, other than by procedures described herein, will be considered as a proxy given to the Chair.

7. Main Activities of the VOLT Standards Committee

7.1. Application for Interoperation via the Virginia Bridge Certification Service

7.1.1. The VOLT Standards Committee, through its Virginia Bridge subcommittee, shall develop a procedure to be used by state entities wishing to apply for interoperation via the Virginia Bridge Certification Service. The procedure shall be approved by majority vote of all voting members and shall cover: (a) how the applicant entity demonstrates that its CA Certificate Policy is equivalent to the VOLT Certification Policy standard respecting certificate levels of assurance; and (b) what duties and responsibilities the applicant entity will have if it is accepted for interoperability with the Virginia Bridge, expressed in the form of a Memorandum of Agreement (MOA) between the VOLT Standards Committee and the applicant entity.

7.1.2. Upon receipt of an application, the VOLT Standards Committee, through its Virginia Bridge subcommittee, shall review the application and make a determination whether to accept it as received, accept it with changes (such as a different policy mapping than the applicant proposes), or reject it. This determination, upon recommendation by the Virginia Bridge subcommittee, shall require at least 75 percent majority vote of the voting membership of the VOLT Standards Committee (excluding any member who must recuse him or herself because he or she represents an entity with a direct interest in the question). All voting members and interested parties shall be afforded an opportunity to review the application and make their views known to the voting membership prior to the vote being taken. Those who oppose accepting the application shall be given a full opportunity to have their concerns heard and discussed.

7.1.3. If the application is accepted without changes, the applicant entity and the Chair of the VOLT Standards Committee shall sign the MOA, and then the Chair shall instruct the Virginia Bridge Certification Service, in writing, to take action to effect interoperability between the applicant entity and the Virginia Bridge Certification Service.

7.1.4. If the application is accepted but with changes required by the VOLT Standards Committee, the applicant entity will be apprised, and if it agrees with the changes, the process in 7.1.3 shall be followed.

7.1.5. If the application is rejected, the VOLT Standards Committee shall apprise the applicant entity of the reasons for the rejection. The applicant entity may then revise its application and reapply without prejudice.

7.1.6. The authority to perform the duties and responsibilities described in 7.1.2 through 7.1.5 may be delegated to the Virginia Bridge Certification Service staff upon recommendation by the Virginia Bridge subcommittee and 75 percent majority vote of the voting membership of the VOLT Standards Committee. Such delegation may be rescinded by a 75 percent majority vote of the VOLT Standards Committee voting membership.

7.1.7. If, subsequent to approval for interoperability, an entity is found to be or admits that it is in material noncompliance with the MOA, the VOLT Standards Committee by at least 75 percent majority vote of the voting membership (excluding the entity in question) shall determine what action to take, which may include termination of interoperability. The entity in question shall have a full opportunity to participate in these deliberations, but shall not cast any votes. The VOLT Standards Committee shall develop procedures approved by majority vote of the voting membership describing how it will perform this function. At their discretion, member entities may cease or restrict interoperability with the affected entity prior to this determination.

7.2. Application for Certificates from the Virginia Central PKI Services vendor

7.2.1. The VOLT Standards Committee, through its Virginia Central PKI Services subcommittee, shall develop a procedure to be used by state entities wishing to issue VOLT certificates. The procedure shall be approved by majority vote of all voting members.

7.2.2. If, subsequent to approval for an entity to use Commonwealth of Virginia certificates, an entity is found to be or admits that it is in material noncompliance with the policy and practices related to such certificates, the VOLT Standards Committee by at least 75 percent majority vote of the voting membership (excluding the entity in question) shall determine what action to take, which may include revocation of all of the entity's certificates. The entity in question shall have a full opportunity to participate in these deliberations, but shall not cast any votes. The VOLT Standards Committee shall develop procedures approved by majority vote of the voting membership describing how it will perform this function. At their discretion, member entities may cease or restrict acceptance of certificates associated with the affected entity prior to this determination.

8. Revisions to Charter

8.1. Revisions to this charter may be made upon at least 75 percent majority vote of the voting membership.

APPENDIX V

DIGITAL SIGNATURES COST MODEL

By Al Carpenter, Department of Motor Vehicles
September 11, 2000

INTRODUCTION

This portion of the report will contain an analysis of the cost elements of initiating and supporting an e-business replacement, using digital signatures for authentication and non-repudiation, for a manual paper process.

Activity-Based Cost: The cost model contained herein is modeled after activity-based costing (ABC) principles. ABC is a method of cost determination that endeavors to properly identify all activities associated with a particular business function, and to then determine the cost associated with each of the identified activities. By using ABC, business enterprises are able to accurately determine the true cost of performing each of their business functions. ABC is often used in reengineering exercises, where identifying business function activity and its true cost are of critical importance in the success of the exercises.

General types of cost included within the Activity-Based Cost Model: Gaining an understanding of the various types of cost is important in understanding the mechanics of the ABC model as it is utilized in this report. The following are the basic cost elements incurred for installing an e-business application:

- *Hardware and software acquisition*: The costs for purchasing the hardware and software.

- *Consulting, installation, configuration, testing*: The costs incurred for initially designing and installing a system, and for testing it.

- *Staffing and training costs*: The costs for any additional staffing time required, as well as training time and expense. This category also includes any costs incurred for reengineering manual processes so that "best practices" are implemented electronically.

- *Facilities*: The costs for any additional facilities or furnishings required.

- *Ongoing maintenance*: The costs for maintaining the hardware and software.

Organizations will incur these costs as either direct costs or opportunity costs.

- A *direct cost* represents an additional out-of-pocket expense for an organization – it has to "write a check" for this cost. An example of this is the purchase of a piece of software that the organization did not use previous to the implementation of a particular e-business solution.

- An *opportunity cost*, on the other hand, is an expense that an organization can absorb using its current assets. The "cost" of an opportunity cost is foregone activity – what an organization has to give up doing in order to take on the new function. One example of an opportunity cost occurs when an e-business function requires a help desk, and the organization absorbs the newly required help desk functionality into a help-desk function that existed prior to assuming the new e-business process.

Opportunity costs have the unique characteristic of being an "opportunity," instead of a "direct" cost only within a relevant range of resources (this is referred to as a "step-cost" in cost accounting parlance). This is true because an existing set of resources is only able to absorb work up to 100% of its capacity. For instance, in the previous help desk example, if the help desk has to hire an additional person because of the anticipated work resulting from a new e-business process, the cost of that additional person is a direct cost. However, the cost of any work assumed by the existing help desk operation is an opportunity cost.

APPENDIX V

COST MODEL

OVERVIEW

Once an organization decides to implement an e-business solution, there are a myriad of alternatives that will affect individual cost components, and therefore, the final cost of the project. Obviously, as the scope of the project increases, either in terms of number of seats, or complexity of the manual process converted to e-business, the cost of the project increases. As a general rule though, as the number of seats increases the per-seat cost tends to decrease, within a relevant range. Until the Early Adopters applications are identified, we cannot estimate the pricing. The Procurement Team and the Department of Information Technology have identified component costs and relative costs, and will work with the Early Adopters candidates to provide firm cost estimates and measure scalability.

Other than the number of seats and project complexity (or maybe even including these items) the decision that has the greatest effect on the cost of any e-business solution (using digital signatures) is whether to in-source or out-source the certificate authority function.

Operating a certificate authority with the proper security is an extremely complicated undertaking in a rapidly-changing technology environment. Because of this, many states are choosing to out-source their certificate authority function as they begin adopting digital signature technology for use in their e-business solutions. A primary driver of the high cost of certificate authority startup and continuing operation is the high level of security required, both physical and systems security. Maintaining a high quality security level for a certificate authority ensures that users of an e-business solution have the highest possible trust in the digital certificates that they receive or send. This is absolutely crucial for the success of the e-business solution employing digital certificates. The AICPA's *WebTrust* **tm** auditing plan is indicative of the large number of security requirements for a certificate authority. This document is discussed more fully in the audit and control section.

Because of the highly complex nature of an in-sourced certificate authority, the potential legal liability involved, and the number of states choosing to outsource their certificate authority operations, the cost model contained herein will presume that certificate authority services are outsourced. However, this does not preclude agencies from in-sourcing their certificate authority services.

COST MODEL AND ELEMENTS

COST ELEMENT	COST: (O)pportunity (D)irect (B)oth	E-BUSINESS ACTIVITY UNIT		
		Registration Authority	**Certificate Authority**	**End-user environment**
HARDWARE AND SOFTWARE ACQUISITION				
Digital signature end-user computer security – • Password • Tokens • Biometrics	D D D			✔ ✔ ✔
Cost for outsourced certificate authority services	D		✔	
Disaster recovery for e-business databases, indices	B			✔

COST ELEMENT	COST: (O)pportunity (D)irect (B)oth	E-BUSINESS ACTIVITY UNIT		
		Registration Authority	Certificate Authority	End-user environment
Integration of e-business database to any required legacy systems or other client/server-based systems	D			✔
Indexing software and/or database software for retaining electronic documents	D			✔
CONSULTING, INSTALLATION, CONFIGURATION TESTING				
Designing and developing e-business solution	B			✔
STAFFING AND TRAINING COSTS				
Registration authority personnel	B	✔		
Time to establish certificate on individual computers	B			✔
Training – dollars to pay for certificate use, e-business system use, and staff time to participate in training.	B			✔
Reengineering – staffing cost for any reengineering exercises undertaken to convert manual systems to electronic	B			✔
Help desk support	B			✔
Assistance for pilot, testing and deployment (including installation on end-use computers)	B			✔
Audit of 3rd party certificate authority provider	D			✔
Audit of e-business solution and security over digital signature certificates on end-user machines	B			✔
FACILITIES COST				
Registration authority facilities	O	✔		
ONGOING MAINTENANCE				
Electronic forms or other interface package	D			✔

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

By Craig Goeller and Charles Lawver, Department of Medical Assistance Services

July 25, 2000

The purpose of the HIPAA Administrative Simplification section is to improve the Medicare and Medicaid programs and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general, by simplifying the administration of the system and enabling the efficient electronic transmission of certain health information. HCFA interprets the Act to direct standards for transferring data elements to apply to the electronic form of the transactions – not the electronic transfer of standard data elements.

BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA) better known as the Kennedy-Kassebaum Bill was signed into law on August 21, 1996. The "Portability" portion dealt primarily with continuation of health insurance coverage and provides for the wavier of pre-existing conditions when persons move to a new employer. During Senate committee sessions on the bill, a section on Administrative Simplification was amended into the original bill for the "Accountability" portion. The Administrative Simplification provisions required that the Secretary of the Department of Health and Human Services (DHHS) develop national uniform regulations dealing with standardization of virtually every facet of electronic commerce related to health care. These proposed regulations include:

1. security of electronic health information and electronic signatures;
2. privacy of such patient identifiable information;
3. standardization of electronic data interchange (EDI) formats of transactions and codes;
4. national provider identifier, and
5. national employer identifier.

The proposed rules apply to any health plan, any health care clearinghouse, and any health care providers that electronically maintain or transmit any health care information relating to an individual. It will require all U.S. health care organizations that transmit or store electronic messages or records pertaining to individual patients (including providers, insurers, and health care clearinghouses) to prevent the unauthorized use or disclosure of such information, while also ensuring easy access for authorized users and approved purposes. This overview will focus on the security and electronic signature and privacy portions of HIPAA

HIPAA SECURITY AND ELECTRONIC SIGNATURE PROPOSED REGULATION COMPLIANCE DATE

Under HIPAA, the Secretary of DHHS was mandated to promulgate security standards for the protection of electronic health information. On August 12, 1998, DHHS published the Security and Electronic Signature Standard in the Federal Register as a Notice of Proposed Rule Making (NPRM) for public comment. Due to the large volume of comments (2,000+) that had to be analyzed, the Y2K remediation effort, and clarifications between the Security and Privacy NPRMs, the final regulation has not been published. It has been announced that it will be finalized by the end of the year. Once the final regulation is published in the Federal Register, there is a 60-day review period by Congress and then it is required to be implemented within 24 months.

APPENDIX W

HIPAA AND ELECTRONIC MESSAGES

Public key infrastructure (PKI) technology is a robust and proven solution for protecting electronic messages communicated over unsecured paths. PKI satisfies both the information security requirements spelled out in the DHHS proposed rules and the health care industry’s unique functionality needs.

- PKI satisfies the DHHS requirements for data confidentiality, user authentication, access control, data integrity, and support for non-repudiation. It encompasses the necessary administrative procedures, physical safeguards, and audit trails that the DHHS rules necessitate.
- PKI satisfies the health care industry’s needs for reliability, open architecture, high availability, scalability, a secure operating infrastructure, and ease of administration.

HIPAA will require all U.S. health care organizations that transmit or store electronic messages or records pertaining to individual patients (including providers, insurers, and health care clearinghouses) to prevent the unauthorized use or disclosure of such information, while also ensuring easy access for authorized users and approved purposes. The regulation requires health care organizations that conduct electronic health care information exchange to:

- Establish clear administrative procedures to ensure the integrity, confidentiality, and availability of information pertaining to individual patients
- Employ technical security services to ensure the integrity and confidentiality of patient data
- Implement physical safeguards to control access to patient information
- Provide for audit trails that record all access to patient information
- Adhere to specified electronic signatures standards, if electronic signatures are used in transmitting such information, to ensure message integrity, authenticate users, and support non-repudiation

The act establishes severe financial and criminal penalties for those who deliberately violate its provisions or ignore its requirements. The civil monetary penalty for violating transaction standards is up to $100 per person per violation and up to $25,000 per person per violation of a single standard for a calendar year. The penalty for knowing misuse of individually identifiable health information can be up to $250,000 and/or imprisonment of up to ten years.

The act also mandates that DHHS enact health privacy regulations by Feb 2002. There are several components to draft privacy provisions including prohibiting persons from improperly using a unique health identifier, obtaining “individually identifiable health information” and disclosing “individually identifiable health information” to another person.

It will be the responsibility of affected organizations to develop a security plan, secure access to electronic records, and train and monitor employees to ensure that they follow the established security protocols. DHHS has intentionally made its proposed rules “technology-neutral”: the rules tell organizations what they must do but leave it up to each organization to decide how best to do it. To avoid tying health care organizations to technologies that may become obsolete in the future, the rules do not require the use of specific technologies. The idea is to leave it up to individual organizations to assess their unique needs and adopt the best solution for their situation.

ADMINISTRATIVE REQUIREMENTS

Paragraphs (c) through (f) of section 1173 of the Act require the Secretary to adopt standards for code sets for each data element for each health care transaction listed, security standards to protect health care information, standards for electronic signatures (established together with the Secretary of Commerce), and standards for the transmission of data elements needed for the coordination of benefits and sequential processing of claims. Compliance with electronic signature standards will be deemed to satisfy both State and Federal statutory requirements for written signatures with respect to the transactions listed in paragraph (a) of section 1173 of the Act.

APPENDIX W

SECURITY STANDARD

- Currently, there is no recognized standard that integrates all the components of security that must be in place to preserve health information confidentiality and privacy as defined in the law.
- The proposed rule would designate a new, comprehensive standard, which defines the security requirements to be fulfilled.
- The security standard must be technology-neutral.
- The security standard must be scalable.
- Health care entities engaged in electronic maintenance or transmission of health information will be required to assess potential risks and vulnerabilities to the individual health data in its possession in electronic form, and develop, implement, and maintain appropriate security measures that will be documented and kept current.
- The proposed rule for security requirements is divided into the following four categories to guard data integrity, confidentiality, and availability:

  1. Administrative procedures;
  2. Physical safeguards;
  3. Technical security services; and
  4. Technical security mechanisms.

However, the proposed rule states that the only necessity is that the requirements are met, not that they are presented in these four categories.

- The security standard met the ten criteria listed in Section (II)(F) of the proposed rule, which were used to evaluate the proposed standard.
- Specifically, the proposed rule requires written procedures to document security compliance with:

1. Administrative Procedures to Guard Data Integrity, Confidentiality and Availability

- Certification, an internally or externally administered technical evaluation that establishes the extent to which a computer system meets a pre-specified set of security requirements.
- A chain of trust partner agreement between any two business partners who exchange regulated data.
- A contingency plan for responding to any system emergency, specifically:
  - Application and data criticality analysis;
  - A data backup plan;
  - A disaster recovery plan;
  - An emergency mode operation plan; and
  - Testing and revision procedures.
- Formal mechanism for processing records.
- Information access control, specifically:
  - Access authorization policies and procedures.
  - Access establishment policies and procedures.
  - Access modification policies and procedures.
- Internal auditing procedures and documentation.
- Personnel security procedures and documentation, including:
  - Procedure(s) for the supervision of maintenance personnel by authorized, knowledgeable persons;
  - Procedure(s) for maintaining a record of access authorizations;
  - Procedure(s) assuring that operating and maintenance personnel have proper access authorizations;

    - Procedures for establishing personnel clearance;
    - Procedure(s) for establishing and maintaining personnel security; and
    - Procedure(s) for assuring that system users and maintenance receive security awareness training.
- Security configuration management procedure(s), including:
    - Documentation
    - Hardware and software installation and maintenance, including review and testing for security features;
    - Inventory procedures;
    - Security testing
    - Complete virus checking.
- Security incident procedures, including:
    - Report procedure(s) to document security incidents, and
    - Response procedure(s) to document security incident record keeping.
- Security management process, including:
    - Risk analysis;
    - Risk management;
    - Sanction policies and procedures; and
    - Enterprise-wide security policy.
- Employee termination procedures,
- Training procedure(s),
    - Security awareness training;
    - Periodic security reminders;
    - User education on security responsibilities; and
    - User education in password management.

2. Physical Safeguards Over Data Integrity, Confidentiality and Availability

- Assigned security responsibility.
- Electronic media control, including:
    - Access control;
    - Accountability, e.g., traceability;
    - Data backup;
    - Data storage; and
    - Data disposal.
- Physical access control, including:
    - Disaster recovery;
    - Emergency mode operation;
    - Equipment control;
    - Facility security plan;
    - Access authorization review and verification;
    - Maintenance records;
    - Personnel access based on "need-to-know;"
    - Visitor and escort control; and

  - Testing and revision.
- Written policy guidelines and procedure(s) on workstation use.
- Secure workstation location(s).
- Security awareness training.

3. Technical Security Services, Guarding Date Integrity, Confidentiality and Availability

- Technical security services must include all of the following:
  - Access control, including:
  - Procedures for emergency access; and
  - At least one of the following:
    - Context-based access;
    - Role-based access; or
    - User-based access.
  - The use of encryption is optional.
  - Audit controls.
  - Authorization controls, including at least one of the following:
  - Role-based access; or
  - User-based access.
  - Data authentication.
  - Entity authentication, including:
  - Automatic log off;
  - Unique user identification; and
  - At least one of the following:
    - A biometric identification system;
    - A password system;
    - A personal identification number (PIN);
    - Telephone callback; or
    - A token system which uses a physical device for user identification.

4. Technical Security Mechanisms To Guard Against Unauthorized Access to Data That is Transmitted Over a Communications Network

  - Communications/Networks controls.
  - Integrity controls.
  - Message authentication.
  - One of the following implementation features:
  - Access controls; or
  - Encryption.
  - If using a network for communications, the following would be required:
  - Alarm;
  - Audit trail;
  - Entity authentication

ELECTRONIC SIGNATURE STANDARD

HIPAA does not require an electronic signature, however, if one is used the proposed rule sets a digital signature standard that includes the following:

- Message integrity;
- Non-repudiation; and
- User authentication.
- The following implementation features are optional:
    - Ability to add attribute;
    - Continuity of signature capability;
    - Countersignatures;
    - Independent verifiability;
    - Interoperability;
    - Multiple Signature; and
    - Transportability.

The proposed rule does not state any enforcement procedures, but will do so in a future Federal Register notice once the industry has some experience with using the standards.

IMPLICATIONS FOR THE COMMONWEALTH

Health care organizations of all types and at all private and governmental levels are becoming more and more dependent upon electronic media. This is so because the sheer volume of health care related data and transactions increases daily and makes automated approaches an imperative for survival in an ever more competitive environment. Throughout the health care domain, paper records and forms are being supplanted by electronic records, which are now routinely transmitted over intranets, extranets and the Internet. The reality of lower costs, greater efficiency, and enhanced quality of care afforded by electronic versus paper-based records and communications in health care is apparent. The Internet, in particular, has the potential to overcome the health care sector's characteristic fragmentation, with a ubiquitous, global infrastructure--accessible at very low cost--for the instant transmission of patient information, consultations between health care providers in far flung locations, and even the filing of health care provider claims. Achieving the potential of electronic messaging is essential to gain patient confidence in today's climate and every Virginia State agency involved with health care is, and will be, involved in ever more electronic approaches and solutions to the challenges of the health care domain.

We all know, however, that there are a group of very important challenges facing any government or private organization using high volume electronic messaging. This group of problems centers around the vulnerability of electronic messages to unauthorized interception and tampering, particularly when they are sent over unsecured paths such as the Internet. Considering the pace at which governments and their business partners involved in the health care sector are adopting electronic messaging for the exchange of information and the highly personal and potentially destructive nature of the information being exchanged, it is troubling to note that the vast majority of today's communications in health care are not secure. If the use of the valuable Internet resource by the health care community and its Virginia governmental partners is to continue and grow, health care information communicated electronically must be secured to ensure that sensitive patient information is carefully guarded to maintain patient confidence. This data must also be secured to protect providers and payers like Virginia Medicaid from liability exposure and possible Federal and legal sanctions.

Acting under pressure from consumer and patient protection groups, Congress moved to ensure the security of health related information transmitted electronically with passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It affects health care providers, health plans and health care clearing houses and directs the Department of Health and Human Services (HHS) to develop information security standards to protect individual health information. It will require all U.S. health care organizations that transmit or store electronic messages or records pertaining to individual patients (including providers, insurers, and health care clearinghouses) to prevent unauthorized use or disclosure of such information, while also ensuring easy access for authorized users and approved purposes.

Virginia State agencies involved in health care and their private partner organizations must establish clear administrative procedures to ensure the integrity, confidentiality, and availability of information pertaining to individual patients. In addition, they must employ technical security services to ensure the integrity and confidentiality of patient data. These organizations must implement physical safeguards to control access to patient information and provide for audit trails that record all access to patient information. If these organizations elect to use **electronic signature technology**, then they must implement specified electronic signature standards to ensure message integrity, to authenticate users and to support non-repudiation.

Very important for governmental entities and their partners, the Act establishes severe financial and criminal penalties for those who deliberately violate its provisions or ignore its requirements. The civil monetary penalty for violating transaction standards is up to $100 per person per violation and up to $25,000 per person per violation of a single standard for a calendar year. The penalty for knowing misuse of individually identifiable health information can be up to $250,000 and/or imprisonment for up to 10 years.

The act also mandates that HHS enact health privacy regulations by February 2002 (it now looks like the final rules on security/privacy will be issued sometime in the Fall of 2000). There are several components to the draft policy provisions including prohibiting persons from improperly using a unique health identifier, obtaining "individually identifiable health information" and disclosing "individually identifiable health information" to another person.

It will be the responsibility of affected Virginia government agencies receiving Federal health care related funding to develop a security plan, secure access to electronic records, and continuously train and monitor employees to ensure that they follow the established security protocols. HHS has intentionally made its proposed rules "technology-neutral"; the rules tell organizations what they must do but leave it up to each organization to decide how best to do it. To avoid tying health care organizations to technologies that may become obsolete in the future, the rules do not require the use of specific technologies. The idea is to leave it up to individual organizations to assess their unique needs and adopt the best solutions for their individual situations.

Although state agencies involved in health care will appreciate the power to assess their own needs, the realities of implementing systems that will satisfy HHS requirements for both security and ease of access is daunting. Furthermore, this task will be hampered by key characteristics of the health care industry, which despite its increasing dependence on technology remains technologically fragmented. Of the seven hundred thousand licensed physicians in the United States, approximately five hundred thousand are in direct patient care practices, and more than 50 percent of these doctors are in independent work groups of less than three physicians. Less than 15 percent of all physician practices have any named or dedicated IT staff or resources. On average, U.S. hospitals have more than forty distinct information systems, handling information for different departments and divisions, and fewer than 35 percent of these systems regularly share information with other systems.

Within Virginia State government, no single entity has yet been assigned overall responsibility for the coordination and implementation of HIPAA compliance across Agency and Secretarial lines. It must not be lost sight of that the bulk of HIPAA compliance related activities (those involving privacy, security and on-going training) will not take place in Information Management departments over the long run (only 15% of HIPAA compliance directly involves IM), so HIPAA is not an IM project...it is an agency wide project. Compliance with the complex security and privacy provisions of this Act will totally change the way Virginia State agencies receiving health related Federal funds do their business in the future. Other State governments, which have been more vocal and involved in the HIPAA compliance process, are currently shaping the environment in which Virginia will soon have to operate. The bottom line is that Virginia State government is faced today with an immediate challenge upon which it is well advised to immediately act.

References

Phoenix Health Systems website at http://www.hipaadvisory.com/regs/finaltrans/index.htm **and its references.**

APPENDIX X

INTERNATIONAL DIGITAL SIGNATURES EFFORTS

September 13, 2000

ARGENTINA

- Presidential Decree No. 427/98, signed by the President of Argentina 4/16/98. This decree authorizes the use of digital signatures for two years within the National Public Sector. Provides legal authority and effect for digital signatures for all public authorities, administrations and government entities.
- Resolution SFP No. 194/98 Secretary of Public Administration - Standards for the Public Key Infrastructure for the National Public Sector of Presidential Decree No. 427/98. Enacted 11/27/98. Implementation limited to the public sector.
- Resolution 212/98 - New Regulation Regarding the Licensing of CAs within the Argentine Federal Government, enacted 12/30/98. Implementation limited to the public sector.
- Web site: http://www:pki.gov.ar

AUSTRALIA

- Federal legislation effective 3/15/00. Royal Assent 12/10/99. Victoria and New South Wales have passed legislation and are awaiting proclamation. All other states and territories have endorsed the federal legislation and are expected to introduce their own statutes in 2000. Generally applicable to all communications.
- New legislation and/or study are currently underway for an Internet Code of Practice and Internet information privacy.
- Web site: http://www.law.gov.au/publications/ecommerce

AUSTRIA

- E-Commerce Task Force studying Internet usage and Internet retail sales. Seven working groups formed to focus on e-commerce.
- Web site: http://www.austria.gv.at/aktuell/database/topnews/english/

BERMUDA

- Electronic Signatures and Records Act passed 7/99. Provides legal force and validity to electronic signatures and records. Applies generally to all communications. Authorizes promulgation of regulations for use, import and export of encryption programs. Sets up an E-Commerce Advisory Board.

BRAZIL

- A special committee of the House of Representatives is finalizing an e-commerce bill based on the UNCITRAL Model Law and originally drafted by the Brazilian Bar Association. This bill would establish minimum security requirements and certification for electronic signatures and documents. The special committee expects the bill to be effective by the end of the year (9/11/00).

CANADA

- Electronic Information and Documents Act passed 6/21/00. Provides legal validity for e-signatures and documents. Exempts certain documents such as wills. Provides for the formation of a contract using electronic signatures and documents.

- Personal Information Protection and Electronic Documents Act passed 4/4/00. Protection for personal and business information on the Internet. Limited to communications with government agencies.
- E-Commerce and Business Use of the Net survey released. Compilation of 1999 e-commerce figures will provide a benchmark for measuring the growth of e-commerce in Canada over time. The study measures the amount of B2B and consumer Internet sales and indicates the degree of connectivity throughout the country, the level of Internet penetration by business, and industry confidence in the Canadian policy and legal framework for e-commerce. (Web site for survey: http://www.statcan.ca/Daily/English/000810/d000810a.htm)
- Canada and the European Union announce a plan to synchronize their e-commerce strategies in order to create an international framework for e-commerce development. (Joint Statement, 7/17/00.)
- Web site: http://www.e-com.ic.gc.ca/

CHINA

- The Shanghai Municipal Bureau for Industry and Commerce issued regulations 9/6/00 that require any Shanghai-registered enterprises or private businesses that operate on-line to apply for an e-digital license.
- The Beijing Municipal Administration for Industry and Commerce has enacted on-line privacy protection regulations 7/24/00.
- An agreement has been formed between Singapore-based bex.com and two Chinese companies to develop China's business-to-business e-commerce software as a national standard.

COLUMBIA

- Electronic Commerce Law (including digital signatures) passed 8/21/99. Establishes the validity of digital signatures and provides standards for licensing certification authorities. It is based on the 1996 UNCITRAL model law.

DENMARK

- Draft Electronic Signatures and Records bill (including digital signatures) introduced 2/16/98. It would apply to all communications. It specifies three models that may be used to give a digital communication legal presence.
- Web site: http://www.fsk.dk/cgi-bin/left-org-main.cgi

ECUADOR

- Draft Electronic Signatures and Records bill (including provision for digital signatures) has been introduced.

EUROPEAN UNION

- A Directive on Electronic Commerce was adopted by the EU 6/8/00.
- EuroCommerce and Eurochambres agree on 6/20/00 to a Code of Conduct for e-retailers; a trustmark (or logo) indicating that an e-retailer belongs to the scheme; and an Online Alternate Dispute Resolution scheme called "Online Confidence."
- EU approves initiative by US and EU banks for standardized E-Signature authentication 8/14/00.
- EU Directive 99/93/EC issued 12/13/99. It establishes a community framework for Electronic Signatures.
- EU directives issued concerning: copyright protection, data protection, privacy, electronic commerce and electronic signatures.

- Web site: http://europa.eu.int/comm/internal_market/en/media/eleccomm/2k-442.htm

FINLAND

- Electronic Service Act effective 1/100. Provides for the rights, duties and responsibilities for administrative authorities and their customers.
- Guidelines issued 10/12/98 on a national cryptography policy.
- Web site: http://www.om.fi/2838.htm

FRANCE

- Electronic Signature bill introduced 9/99.
- Two-year committee formed 12/14/99 to enhance e-commerce.

GERMANY

- Information and Communication Services Act passed 6/13/97. It Includes provisions for data protection and digital signatures and an article entitled the Digital Signature Act. It establishes requirements for licensing of certification authorities, and addresses issuance and content of certificates.
- Digital Signature Ordinance enacted 11/1/97 as a result of passage of the Digital Signature Act referenced above. It defines the duties and requirements for certification authorities and establishes fees and procedures for certificate issuance.
- The government announced on 7/5/00 that it intends to introduce over 15 bills relating to and affecting e-commerce in the current legislative session. Included in these bills will be amendments to the Digital Signature Act as a result of the EU Directive on Electronic Signatures.

HONG KONG

- Electronic Transactions Ordinance was enacted 1/7/00. It includes provisions for electronic and digital signatures as well as electronic records. It provides for the legal validity of digital signatures and electronic records. In addition, it defines requirements for formation of an electronic contract.
- The Hong Kong Monetary Authority issued initial guidelines for e-banks 5/16/00. It is requesting comment on the guidelines, which would define requirements and restrict e-banking to existing, previously licensed lenders. Any on-line bank would have to be owned by an established bank and have a physical presence in Hong Kong.

INDIA

- The Information Technology Act was passed by the Indian Parliament 5/00 and assented to by the President 6/19/00. It provides legal recognition for electronic transactions and records and for digital signatures. It further establishes a Controller of Certifying Authorities as well as a Cyber Appellate Tribunal.
- The Union Government is establishing a committee to create e-commerce standards. This would include building standard roadmaps for e-commerce with private sector companies, providing technical assistance to the industry in the development and harmonization of open standards in e-commerce, establishing neutral test beds and developing pilot projects in e-commerce with technical experts from the private sector.
- The Madhya Pradesh Government issued a State Policy on Information Technology, which establishes guidelines and principles for participation and investments in e-governance projects for citizen services. The scope of e-governance projects would also include development of databases and contents,

processing of information required for such services, designing of application software and use of hardware.

IRELAND

- The electronic commerce bill 2000 was passed 7/10/00. It provides for the legal validity and enforceability of electronic records and signatures. It protects users of encryption and forbids law enforcement from demanding the encryption keys.

ISRAEL

- The Minister of Justice published the proposed Electronic Signature Bill 5760-2000. It provides for a register of authorizing entities that will be entitled to issue electronic signatures.

ITALY

- The Digital Signature Legislation (No. 59, Art. 15, c. 2) was enacted 3/15/97. It provides for the legal validity of e-documents.
- The Presidential Decree No. 513 issued 11/10/97 provides regulations that expand on the provisions of the Digital Signature Act. The regulations provide for the legality and enforceability of digital signatures
- Rules regulating the registration of certification authorities were enacted 4/15/99.

JAPAN

- An Electronic Signatures and Records bill was enacted 5/24/00, with an effective date of 4/1/01. The bill presumes that electromagnetic documents are authentic, defines electronic signatures and provides for accreditation of certification providers.
- The Financial Reconstruction Commission is set to approve Japan's first Internet bank, led by Sakura Bank.

MALAYSIA

- The Digital Signature Bill of 1997 was passed effective 10/1/98. It establishes the legal validity and enforceability of digital signatures. It authorizes establishment of a Controller of Certification Authorities and provides for annual audits of licensed certification authorities.
- A bill to protect personal data and ensure privacy is in final draft stages and will likely be introduced into Parliament at the end of the year.
- The Communications and Multimedia Commission will implement a simpler licensing structure for companies providing Internet and value-added multimedia services.

MEXICO

- Proposed modifications to the Commercial Code were introduced 4/28/99. The modifications would limit the electronic signatures to only those transactions covered by the Commercial Code.

NEW ZEALAND

- Government E-commerce summit scheduled for November. E-government web site has been launched (web site: http://www.ecommerce-summit.govt.nz/).
- A proposed Electronic Transactions Bill may be revised by the government to specifically include transactions between citizens and government. The proposed bill would provide for legal recognition of digitized signatures and electronic documents.
- Web site: http://www.med.govt.nz/pbt/infotech.html

PAKISTAN

- An Information Technology policy and action plan draft is ready for presentation to the Ministry of Science and Technology, which will present it to the Cabinet for approval. This plan will facilitate and encourage the private sector's development of information technology and telecommunications.
- The Task Force for E-government announced that the process of setting up E-government will be completed by December 2001. A short term program was submitted to the government last week outlining plans for the computerization of all available data and the creation of websites for all government ministries.

PERU

- Draft bills dealing with electronic signatures have been submitted for review.

PHILIPPINES

- Electronic Commerce Act of 2000 (Senate Bill 1902) was enacted 6/14/00. It provides recognition of the authenticity and reliability of electronic data and legal validity for digital signatures and electronic documents. It includes punishment e-commerce-related crimes.
- Electronic Commerce Act of 2000 (House Bill 9971) has been referred to the Senate. The provisions of this bill are limited to Limited to government-issued licenses, permits and other official documents. It also provides for the legal validity of digital signatures and electronic documents.

RUSSIA

- Russian Federation Information Act No. 24-FZ was adopted by the Duma 1/25/95. It establishes the legal validity and enforceability of electronic documents, and of electronic signatures only when the automated system contains the technical means making it possible to identify the signature.

SINGAPORE

- Electronic Transactions (Certificate Authority) Regulations of 1999, issued 2/10/99, govern actions of certificate authorities. They address application procedures and renewal of licenses. Other requirements include compliance audits, types of certificates that may be issued, and renewal, suspension and revocation criteria.
- Electronic Transaction Act of 1998 was enacted 6/29/98. It establishes the legal validity, enforceability and admissibility of electronic and digital signatures, as well as electronic records. It also addresses the liability of network service providers.
- Information Security Guidelines issued 9/99 address information technology security issues and provide policies and guidelines covering security management, system integrity and controls, and physical and operational security. Security Guidelines for Certificate Authorities issued at the same time, cover much the same areas but are directed to companies and organizations functioning as certificate authorities.
- E-Government Action Plan published 6/20/00.
- Web site: http://www.ec.gov.sg/

SOUTH KOREA

- Basic Law on Electronic Commerce enacted. It establishes the validity and enforceability of digital signatures, as well as the validity and admissibility of electronic messages. It authorizes the government to designate a certification authority, and establishes the Electronic Commerce Promotion Program, the Policy Committee on Electronic Commerce, the Korea Institute for Electronic Commerce, and the Electronic Commerce Service Center.

SPAIN

- Two Royal Decrees recognize the legality of electronic signatures. Effective 2/29/00 and 9/17/99.

THAILAND

- An Electronic Transactions Bill has passed its first reading in Parliament 8/29/00. This proposed bill combines two previously separate laws, the Electronic Transaction law and Electronic Signature law and plans for a single regulatory body to control both digital signatures and all e-commerce activities.

UNITED KINGDOM

- The House of Commons passed the Electronic Communications Act of 2000 1/26/00, and Royal Assent was received 5/25/00. This law provides for the legal validity and enforceability of electronic signatures and authorizes the Secretary of State to approve cryptography support services providers. It also contains restrictions on the disclosure of information.
- The Stationary (Post) Office and Compaq Computer have jointly developed a UK Code of Practice for e-business. It covers areas such as laws on data protection, copyright, contracts and computer misuse.
- The Department of Trade and Industry releases a report on electronic commerce, a statement on the legal framework for secure electronic commerce, and a paper on its intent to regulate use of encryption on public networks.
- Web site: http://www.foresight.gov.uk/

APPENDIX Y

ATTRIBUTE CERTIFICATES

By Sally Fehn, Department of Information Technology
August 10, 2000

DEFINITION

Attribute certificates are a mechanism for extending the attributes of an identity certificate. They allow the separation of uses for the identity certificate for authentication and the attribute certificate for authorization (permission). The attribute certificate has no associated key pair itself, but it is securely bound to the identity certificate. Attribute Certificates follow a standard format and can be acquired and verified using protocols and mechanisms currently being standardized in various forums. The International Organization for Standardization (ISO) has defined the basic Attribute Certificate definitions and the Internet Engineering Task Force (IETF) is currently profiling these definitions for use in Internet environments.

Attribute certificates typically have a shorter lifetime than identity certificates. They contain properties such as role-based access, context-based access, emergency-based access, or user-based access that are true about the owner of an authentication (identity) certificate. The AC can be used to securely hold a user identity and password required to access a particular system. This class of attribute is likely to be of particular use for legacy systems and single sign-on applications. Obviously, attributes about people change more frequently than their identities so storing them in a separate certificate with a set lifespan prevents the creation of unwieldy Certificate Revocation Lists (CRLS).

ISSUING ATTRIBUTE CERTIFICATES

An X.509 identity certificate is typically issued by a central (possibly government-run) authority, which enjoys widespread trust within the user community, and has to operate under tightly controlled, and monitored, terms and conditions. Therefore, this entity’s relationship with a user will be distant and formal, with an identity certificate only being issued on production of a defined set of documents, and through a defined process.

An authority that has intimate knowledge of a user’s rights and privileges within a particular community, on the other hand, should issue an Attribute Certificate. In a commercial context, this places the Attribute Certificate issuer firmly within the user's close organization affiliations. Moreover, where short lifetime attribute certificates are used, they must be issued very frequently, and they must accurately reflect changes in these rights and privileges.

Typically, therefore, a central body, external to the organization, will issue a user’s identity certificate, which is broadly trusted within the community. However, the user's attribute certificate(s) will be issued by the organization employing the user, or the organization relying on the access control attributes, and will be issued on a regular, automatic or semi-automatic basis.

HOW TO USE ATTRIBUTE CERTIFICATES

A typical scenario for the use of Attribute Certificates would be in web access, where a standard secure session is established between a browser and web server. For certain resources, the web server requires some proof that the user is, for example, an accountant. One model for doing this is for the web server to query an Attribute Certificate server. The Attribute Certificate returned to the web server contains a set of privileges for the user, so that the required access decision can be made. This mechanism supports authorization in the extremely large systems that will become common once legacy applications are moved to the Internet.

Other potential applications for using Attribute Certificates include:

- VPN access
- FTP access

- Mail access
- Mobile IP access
- Physical access to buildings
- Approval Limits on Purchase Orders
- Security Clearance
- Access according to location
- Membership access / Cert expires on renewal date
- Subscription access / Cert expires on renewal date
- Emergency access relying on credentials
- Session access
- Per-day access

The storage of Attribute Certificates depends largely on the application, the validity period of the certificate, and whether it is obtained and defined directly by the end-user or created for the end-user. If it is a short-lived user-created certificate, the Attribute Certificate may be stored on the client machine and "pushed" by the client to the application on the server. If an administrator for the end-user creates the Attribute Certificate, it may reside in an LDAP directory where it has been published. The application would "pull" the Attribute certificate from the LDAP directory after the identity certificate as been verified and then perform the Access Decision Function (ADF). In all cases, the Attribute Certificate is issued and maintained by an Attribute Authority (AA).

CONCLUSION

Attribute Certificate technology provides a scalable, fine-grained access control tool across multiple platforms and corporate boundaries. They are a standardized mechanism to extend the Public Key Infrastructure so that a centralized administrator can manage users and privileges locally.

References:

Baltimore Technologies

SSE

Netscape

POSITIONING THE COMMONWEALTH FOR SINGLE SIGN ON

By Richard Gill, RSA Security, Inc.
August 9, 2000

WHEN TO SSO AND WHEN NOT TO SSO

The first consideration for a project of this magnitude is to understand that there will be some cases where an application will not lend itself well to achieving SSO. The reasons will be unique for each instance but there are some general guidelines that have proven consistent over the past few years.

1. The application is considered to be of little use beyond a predictable period of time and therefore does not warrant the investment.
2. The application is used by a relatively small population and does not justify the effort.
3. You do not have access to the necessary components of the application in order to achieve SSO.
4. The modifications required represent an extensive technical challenge or a decrease in the application effectiveness.

Having said this, it is reasonable to assume that roughly eighty percent of your applications can be configured to support SSO. Because of this it is probably fair to state that eighty percent does not represent true SSO but rather reduced sign on. This is a quibble and I will refer to the general concept as SSO throughout the paper.

DIGITAL SIGNATURES AND PKI

We must then consider the actual concept the Commonwealth is working on with the Digital Signature initiative. It can be fairly stated that all functioning Public Key Infrastructure (PKI) initiatives contain a digital signature component however, not all digital signature initiatives represent a full PKI, and SSO cannot be achieved without the benefits of a more robust PKI facility.

The distinctions for this are many, and it is important to recognize the limitations of each component. A certified public/private key pair (cert) used for digital signature needs to be issued to a user in a manner that prevents it ever being compromised. The reasons for this are as much legal as technical. The primary purpose of a digital signature is to give legal status to electronic commerce by providing a basis for document integrity and non-repudiation. Therefore, the practical utilization of this key pair should be limited only to the person for which it was originally intended and never recovered or made available to even an administrative authority if its validity is to remain unchallenged.

On the other hand key pairs (certs) that have been issued for purposes of authentication and encryption will be issued as required by the ongoing needs of a particular user and may be issued and/or revoked as the needs of an organization dictate. A simple example of this would be the case of an employee that has left the employ of the Commonwealth. It would be imperative that the Commonwealth be able to decrypt any documents encrypted by the employee in order to understand and make use of the information involved with the document. However, in order for the information to be considered valid then the signature portion must be verifiable without concern for compromise.

These two functional areas generally dictate that organizations issue certs that are created for a specific set of purposes rather than trying to make a signature key pair function for a wide range of applications.

PKI AND SSO

Two primary functions of a properly initiated PKI are user Authentication and Authorization. It is primarily the Authentication component that enables SSO in a PKI environment. However simply having a cert on your desktop does not enable SSO. The cert must be available to the user for the purpose of SSO and, the application must be able to recognize the cert as a user credential.

There are several methods employed for storing certs in order to make them available for a user in an SSO environment.

1. They may be stored in a web browser such as Internet Explorer or Netscape. While this is the most common form of deployment to date this method does not create the most functional or secure environment as the desktop is subject to tampering. Additionally, this method "ties" the credentials (and therefore the user) to a single machine. Finally, in order to achieve SSO, all target applications would have to be "web" enabled. Many applications can easily be web enabled but many more cannot.
2. The certs may be stored in a secure (third party) "credential store" on the desktop eliminating the tampering issue and enhancing functionality interoperability and mobility for the user. This is generally accomplished by storing the credentials on a secure server and having the user authenticate to a specific desktop by using a strong two-factor authentication mechanism.
3. They may be stored on smart cards, which also give the user the advantages of item two above with the benefit of added security.

There are several methods for enabling applications for the use of certificates in an SSO environment.

1. The application can be enabled to support a web based user interface that will accept certs as a form of authentication. As stated above some applications lend themselves easily to this form of modification and some don't.
2. The application could be PKI enabled through a third party facility such as RSA's BSafe line. This approach generally requires access to the source code for the particular application, which may or may not be available.
3. API driven tool kits that allow an application to be wrapped for the purposes of authentication and session security. These usually require some access to source but the nature of the access is usually available to most organizations.
4. Proxy Servers also allow PKI enabling for applications that are not suitable to some of the above-mentioned facilities, or systems managed by third parties where you have, limited access.

There are several more methods for enabling SSO without necessarily using certificates.

1. Creating a small script capable of accepting user variables to log a person in to an application through terminal emulation.
2. Providing mechanisms that support the use of non-PKI tokens and passtickets as a method of authentication.

In order for SSO to become a reality then some combination of the above general scenario will be necessary.

The foregoing issues aside the other issue has to be the actual use of certs in an SSO environment.

Certificates generally fall under the ISO/IEC/ITU/ X.509 standard version 3. This version was created with the purpose of providing certain "extension" fields to the certificate in order to facilitate additional identification of certificate holders and/or functionality to applications and services. Many of the extension fields are called out in the X.509.v3 standard and contain consistent information, however, there are some fields that are left unspecified which are used by the different certificate authorities for locally specific applications/services. The result of this is that a certificate authority can factually state that they are compliant with X.509.v3 while creating certificates that cannot be used by similar PKIs. This represents a barrier to progress because the acceptance of the technology will be predicated on the ability of many small implementations to be aggregated into a very large whole. An example of this would be having only one method of getting to the Internet.

CONSIDERATIONS FOR FUTURE SSO

All of the previous discussion has been provided as a small amount of background regarding the tie in of PKI with a future SSO program. Consequently much of the information is general in nature and each topic can (and should) be explored in much depth of detail.

However, in order to answer the original question I offer the following thoughts regarding getting to SSO from Digital signatures.

1. Begin your deployment with the end in mind; by recognizing that the infrastructure you are building to support digital signatures will have to be expanded almost exponentially in order to cover the range of applications covered under SSO.
2. Recognize that in order to get digital signatures to the desktop you will have to enable your systems to support them. SSO will also require desktop and server components if it is to work successfully. These components may be in addition to what you already have. I recommend that you look for solutions with components that support the full range of PKI functionality, from digital signatures though SSO to avoid having to go through the same effort twice.
3. The desktop/server components you select will have to be able to support digital certificates as well as more mundane access methods such as; user id and password, token and future authentication methods such as smart cards or biometrics.
4. Not all certificates are created equal and you should demand that your chosen vendor guarantee that the certificates they deploy support unencumbered interoperability with other vendor systems. I cannot stress this enough. Consider for a moment that even if the Commonwealth was wildly successful in a deployment with a single vendor the State of Maryland may have the same success with another vendor. When the time came to execute cross boundary functionality a proprietary system will cause just that much more resistance to success.
5. Involve everyone from the beginning. SSO covers all of the geopolitical boundaries within an organization (workstation, network, client server, mainframe and web) and to begin the planning without the input of all involved is to spend the rest of your life explaining the same things over and over.
6. Choose your area of pain and start small. The best place to start is with the people that have the most to gain i.e. many applications requiring secure logon. By doing this you will have found a willing partner that wants you to succeed and you will be praised for incremental gains rather than damned for insufficient progress.
7. Investigate the different methods to achieve your real needs. Look for vendors with solutions that go beyond the absolute in high tech and offer many tools to accomplish the goal. In many cases you may only require a bit of scripting in order to achieve SSO to a particular application. Many will say that scripting is bad, but if it is all you need who cares what “they” say.
8. Don’t try to do everything but definitely avoid “do nothing”. In the final analysis the practicality in trying to bring everything into an SSO environment usually defies logic and practicality. This to some is a reason to do nothing which is the ultimate barrier to progress. SSO isn’t the easiest thing to do but it can be done, and is worth doing in the correct environment.
9. Don’t set arbitrary deadlines (except in geologic terms). Implementing an SSO project tends to bring out the minutia in any system and usually does so just after you have forecast a completion date. Said minutia generally expands the scope of the project which is why the start small rule is one of the best because small problems can be encompassed more easily and progress maintained.
10. Find some form of relaxation such as yoga or meditation. You will be a pioneer and may find yourself a bit frustrated from time to time.

APPENDIX AA

DIGITAL SIGNATURES HORIZONS ISSUES
October 2000

ACCESS CERTIFICATES FOR ELECTRONIC SERVICES (ACES)

In February 1997 Vice President Gore and the National Performance Review issued the report *Access America: Reengineering Through Information Technology*. This report presented a broad plan to provide for widespread electronic access to government information and services using the Internet and other communications systems available to the public. In January 1999 Vice President Gore announced the Access America for Students program to provide such electronic access to the post-secondary student, school, and lending communities. The Access America for Students program is directed through a Steering Committee comprised of twelve federal agencies and chaired by the Office of Management and Budget and the Department of Education Office of Student Financial Assistance. The Steering Committee oversees the work activities of an inter-agency task force. The implementation of common electronic services delivery through ACES is a key goal of the Access America vision and planned activities. The July 30, 1999 *Access America for Students Strategic Plan* is provided as an addendum to this statement of work for reference.

In October 1998 the Government Paperwork Elimination Act (GPEA) was signed into law. The GPEA calls for Federal agencies to provide individuals and entities that receive services or business with the government to provide for the electronic submission of information or electronic transactions to replace paper-based processes by October 2003. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability, and specifically sanctions Federal government use of a range of electronic signature alternatives. The agencies seeking to obtain services through this task order are planning to provide broad based electronic service availability to comply with GPEA requirements and directives.

Following is a brief description of the agency applications planned for pilot testing with ACES.

- **U.S. Department of Education: Free Application for Federal Student Aid (FAFSA)**

  The Department of Education receives 14 million federal student aid applications (FAFSA) annually and plans to move the entire process on-line. The Department currently supports on-line FAFSA renewal applications using PIN authentication. The Department is in the process of issuing authentication PINs to support online FAFSA applications and systems access to approximately 14 million student aid applicants in calendar year 2000. It is the goal of the Department of Education to replace the PIN based process for electronically signed FAFSA with PKI based digital signature. To gain experience and assess the digital signature application for FAFSA, the Department of Education seeks to pilot test using ACES for digitally signed FAFSA applications on-line. (See the web-based FAFSA application at http://ed.gov.

- **U.S. Department of Labor: America's Learning Exchange (ALX) Career Management Account**

  The Department of Labor Education and Training Administration (ETA) administers America's Career Kit -- the most comprehensive employment resource on the Internet. America's Career Kit includes America's Job Bank, America's Talent Bank, America's Career InfoNet, and America's Learning eXchange (ALX). As part of the ALX, the Labor Department ETA is creating individual Career Management Accounts (CMAs) to provide workers and students with a lifelong learning portfolio and a suite of on-line career management tools. The Department of Labor ETA projects an initial pilot program of 10,000 Career Management Accounts. Authenticated access and disclosure authorization is required for each account. Each account holder will be issued an ACES certificate for digital signature access to and disclosure from their account. The pilot test period is projected from May – October 2000. Based on the pilot test, the Department of Labor intends to offer Career Management Accounts to up to 1.8 million current registrants.

- **U.S. Department of Veteran Affairs: Web Automated Verification of Enrollment WAVE), NetCert, and Electronic Application for VA Education Benefits**

  WAVE: The Department of Veterans Affairs administers veterans benefits programs for veterans enrolled in post-secondary educational institutions. The VBA requires a monthly certification from each veteran of current enrollment status in order to authorize benefit entitlement. Every month an average of 150,000 students receiving VA benefits must verify their enrollment before an electronic fund transfer of their benefit is made. Currently the VA prints and mails the student a monthly verification of enrollment form, which must be returned by mail and manually processed by the VA prior to releasing payment. WAVE will allow a student to electronically verify his or her enrollment every month over the Internet. The information the student provides will be used to electronically process the transfer of benefits due. Each veteran in the pilot program will be issued an ACES certificate to provide for digital signature of the monthly certification. The target date for WAVE availability is April 1, 2000.

NetCert: The VA also requires schools to provide certification of veterans' enrollment in order to authorize veteran benefits entitlement. The VANetCert project will provide educational institutions the ability to electronically submit student enrollment information to VA. The institution can also view a portion of the student record maintained by VA. This will allow them to answer students' questions concerning the amount of status of the VA benefit. The NetCert project will provide educational institutions the ability to electronically submit student enrollment information to VA. The institution can also view a portion of the student record maintained by VA. This will allow them to answer students' questions concerning the VA benefit. The electronic information received from the educational institutions will be transferred directly into another system (TEES, The Education Expert System) which will automatically process the enrollment information without human intervention). School officials in pilot schools will be issued ACES certificates to provide for digital signature for certification of school enrollment. The target date for VANetCert availability is April 1, 2000.

VONAPP: This initiative will create an electronic application for VA education benefits to replace the paper applications now being filed by veterans. The electronic version of the application will provide for on-line submission of the VA application for education benefits (VA Form 22-1990), as well as on-line applications for Compensation and Pension benefits (VA Form 21-526) and Vocational Rehabilitation

Veterans Health Administration (VHA): As part of the planning and support services for the Department of Veterans Affairs, the VHA is also requesting services under this task order. The VHA seeks support to implement test applications during calendar year 2000 to help to meet GPEA requirements.

- **US Postal Service Electronic Change of Address.**

  The US Postal Service National Customer Support Center plans to pilot test electronic change of address using multiple methods of authentication, including ACES certificates for authentication and digital signature. The National Customer Support center for Address Management is located in Memphis, Tennessee and is responsible for managing change of address data and distribution nationwide. Over 40 million Americans change addresses annually. The principal means for obtaining address changes is through the USPS Change of Address Form 3575, which is submitted at local post office locations. The Postal Service offers Internet access through MoversNet (http://usps.com/moversnet). This represents an expanded Internet version of the hardcopy Mover's Guide designed to offer increased help to consumers before, during and after they move to a new address. MoversNet currently allows the public to enter change of address information on the web-based form and to print the completed Change of Address form for delivery to the local post office. The national Customer Support Center intends to pilot test using digital signature to accept electronic change of address form submissions and act on the submitted data directly. USPS operates MoversNet cooperatively with Targeted Marketing Solutions, Inc. (TMSI). This cooperative effort between the private sector and the Postal Service reduces postal operating costs and is part of an ongoing commitment by the Postal Service to use new technology in ways that improve service and convenience for you while reducing costs.[1]

DMV AS A REGISTRATION AUTHORITY

BY MICHIE LONGLEY, DEPARTMENT OF MOTOR VEHICLES
SEPTEMBER 13, 2000

A Registration Authority (RA) verifies user requests for a digital certificate and tells the certificate authority (certificate authority) to issue it. In order to do this, the RA must first ascertain a person's identity and then collect sufficient information about that person to certify their identity before an electronic certification is issued to that person. As this is generally the same process used by a DMV before issuing a driver's license, the idea has been raised that a DMV is in the best position to serve as a state's central RA. To date, California is the only state actively pursuing this proposal as a result of proposed legislation that subsequently failed (California Assembly Bill 2163).

Any DMV considering such a proposal should first examine a number of policy, operational and support areas: levels of assurance in its existing identification verification process, liability issues, program funding, fee structures, staffing needs, privacy concerns, IT system configurations, and data security and audit processes. Overall program design and policy issues must also be identified and resolved. For instance, the scope, extent and responsibilities must be determined. Will the DMV serve as the RA for all citizens and businesses? Will the DMV only verify identity and pass the information to a contractual agent that serves as an RA? Will the certificate be issued as an integral part of the licensing process, or will it be a stand-alone transaction? The California DMV has just begun addressing such issues. It has so far identified legislation and liability as major issues, and had begun to involve legal staff in all phases of the process.

ELECTRONIC FORMS

BY DAVID BUNN, DEPARTMENT OF MOTOR VEHICLES
SEPTEMBER 7, 2000

The ability to obtain the greatest value from E-Forms will depend on how it is architecturally positioned into the environment. The following are recommended architectural components:

1. Deliver forms via an Intranet: The E-Form should be accessible from a Web-Server to provide a central point for access and a single point for version management. The form should be distributed through a browser. This substantially reduces the overhead required to manage form releases and updates to the desktop.
2. Provide interoperability to PKI structures: The installed E-Form product should provide the ability to digitally sign the server-based form, without being restricted to a specific PKI vendor. It should be able to use the signing key regardless of whether it is stored in the browser, client software or a hardware token. It should support the signing of individual fields or the whole document, multiple signatures and archival of the form along with the contents. It should be able to do auto-verification of the signature and CRL checking of all the certificates in the trust path.
3. Support XML: The E-Form product should utilize XML to promote its ability to interface with other applications as they are developed. Note that while XML is standards based, it doesn't function on the same standard level like HTML; each vendor's implementation will require a proprietary viewer for the XML form.
4. Provide interoperability to back-end databases: The E-Form product should support back-end database integration using ODBC.

E-Forms packages are generally not end-to-end business solutions in and of themselves; they are a component of this solution. The E-Forms package will need substantial attention to integrate with the existing technical infrastructure (network, server architecture and back-end database); with the PKI facility that will be operating; with a workflow or routing mechanism to provide user notification and prompting; and to a data warehousing or document management system to provide archival handling.

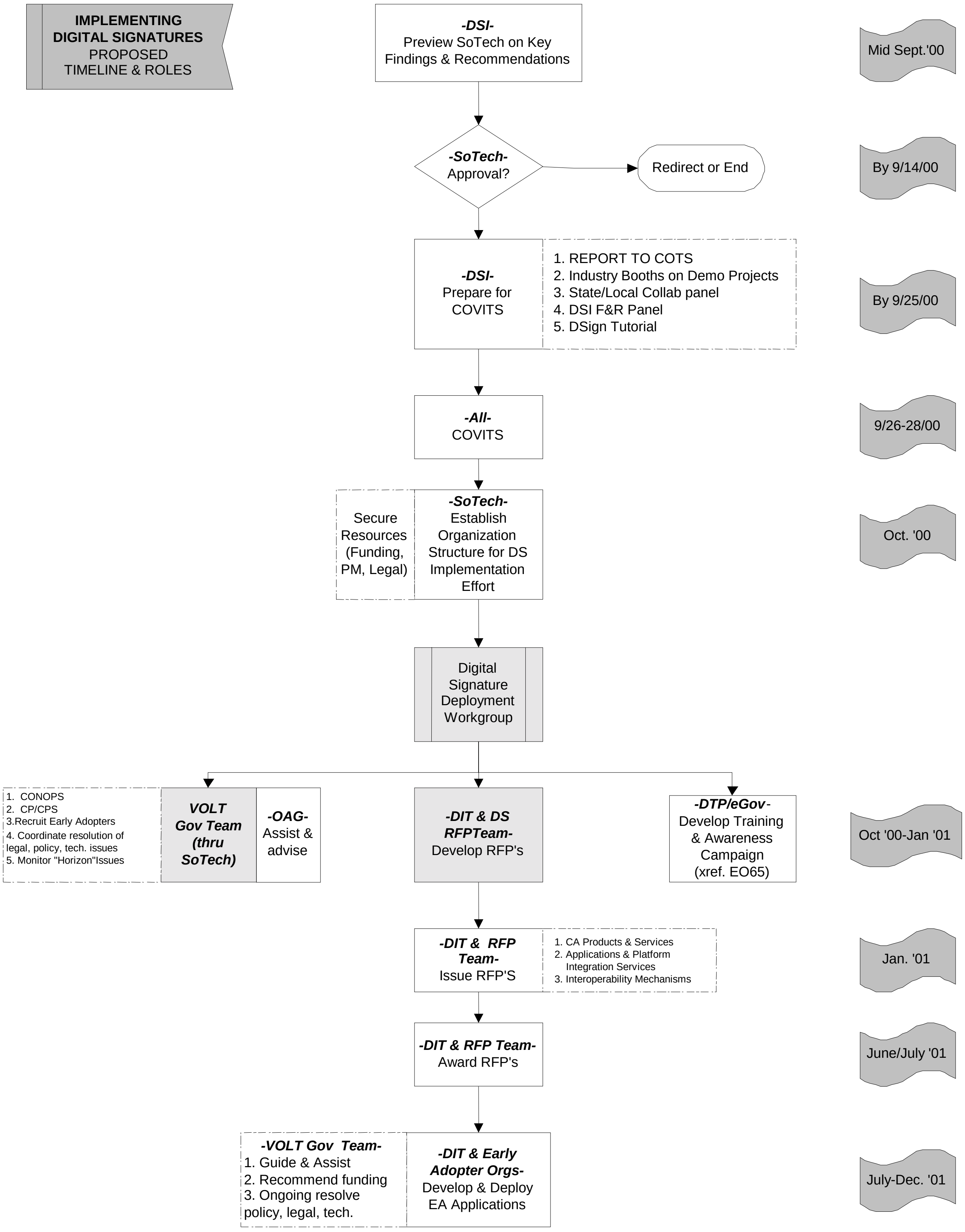
Note:

- While E-Forms packages have developed substantial interoperability with PKI structures and to back-end databases, they do not interoperate with each other: A form developed with one vendor's software does not function in another vendor's environment.

[1] General Services Administration. "Request for Quotation (RFQ) for Planning and Support Services for the Implementation of ACES."

TIME-PHASED ACTION PLAN

SEPTEMBER 25, 2000


IMPLEMENTING DIGITAL SIGNATURES
PROPOSED TIMELINE & ROLES
-DSI-
Preview SoTech on Key Findings & Recommendations
Mid Sept.'00
-SoTech-
Approval?
Redirect or End
By 9/14/00
-DSI-
Prepare for COVITS
1. REPORT TO COTS
2. Industry Booths on Demo Projects
3. State/Local Collab panel
4. DSI F&R Panel
5. DSign Tutorial
By 9/25/00
-All-
COVITS
9/26-28/00
Secure Resources (Funding, PM, Legal)
-SoTech-
Establish Organization Structure for DS Implementation Effort
Oct. '00
Digital Signature Deployment Workgroup
1. CONOPS
2. CP/CPS
3.Recruit Early Adopters
4. Coordinate resolution of legal, policy, tech. issues
5. Monitor "Horizon"Issues
VOLT Gov Team (thru SoTech)
-OAG-
Assist & advise
-DIT & DS RFPTeam-
Develop RFP's
-DTP/eGov-
Develop Training & Awareness Campaign (xref. EO65)
Oct '00-Jan '01
-DIT & RFP Team-
Issue RFP'S
1. CA Products & Services
2. Applications & Platform Integration Services
3. Interoperability Mechanisms
Jan. '01
-DIT & RFP Team-
Award RFP's
June/July '01
-VOLT Gov Team-
1. Guide & Assist
2. Recommend funding
3. Ongoing resolve policy, legal, tech.
-DIT & Early Adopter Orgs-
Develop & Deploy EA Applications
July-Dec. '01